Institut für Maschinentechnik – Lehrstuhl für Fahrzeugtechnik

der

Technischen Universität München

Funktionale Sicherheit von mechatronischen Systemen bei mobilen Arbeitsmaschinen

Marcus Alexander Martinus

Vollständiger Abdruck der von der Fakultät für Maschinenwesen der
Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs

genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr.-Ing. B.-R. Höhn

Prüfer der Dissertation:

1. Univ.-Prof. Dr.-Ing. Dr. h.c. K.-Th. Renius, i. R.
2. Univ.-Prof. Dr.-Ing. B. Heißing

Die Dissertation wurde am 20.09.2004 bei der Technischen Universität München eingereicht und durch die Fakultät für Maschinenwesen am 06.12.2004 angenommen.

Vorliegende Arbeit erscheint auch im VDI Verlag als Fortschritt-Bericht der Reihe 12.

Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als Wissenschaftlicher Mitarbeiter und Assistent am Lehrstuhl für Landmaschinen, ab September 2003 am Lehrstuhl für Fahrzeugtechnik der Technischen Universität München. Mein erster Dank gilt daher meinem verehrten Lehrer und Doktorvater Herrn Professor Renius für die wertvolle fachliche Unterstützung und die freundliche Art seiner Betreuung. Meine besondere Wertschätzung gebührt der von ihm gewährten Freiheit und dem damit verbundenen Vertrauen beim Arbeiten an einem höchst interessanten Forschungsthema.

Vielen Dank Herrn Prof. Heißing für die Übernahme des Koreferats und Herrn Prof. Höhn für die Leitung der Prüfungskommission sowie der mündlichen Prüfung im Dezember 2004. Herrn Prof. Heißing danke ich darüber hinaus für die unkomplizierte und reibungslose Aufnahme der „alten LTMler“ in seinen Lehrstuhl und die damit verbundene Möglichkeit die Forschungsprojekte weiter zu führen.

Ein herzliches Dankeschön an alle meine Kollegen. Ihre Anregungen, Hilfestellungen und stets konstruktive Kritik trugen erheblich zum Gelingen der Arbeit bei. Ganz besonders danke ich Herrn Freimann für die gute Zusammenarbeit. Seine weit blickenden Ideen waren Grundvoraussetzung für dieses Projekt, sein fachliches Wissen und Organisationstalent stets ein Vorbild. Allen FTM-Kollegen danke ich für die nette Aufnahme in ihr Institut. Sie haben uns den Wechsel aus der „LTM-Familie“ durch eine besonders freundschaftliche Atmosphäre wirklich leicht gemacht.

Allen Mitarbeitern der mechanischen und elektrischen Werkstatt danke ich für die umfangreiche Unterstützung bei der Ausrüstung des Versuchsträgers, sowie den Mitarbeitern aus Sekretariat und Technik für die nette Zusammenarbeit. Natürlich möchte ich auch allen Studenten Dank sagen, die als Hiwis, Semestranden oder Diplomanden einen wichtigen Teil der Arbeit für sich einnehmen.

Vielen Dank den Firmen AGCO-Fendt und Lemken für die Stellung des Versuchsgespanns und der Deutschen Forschungsgemeinschaft für die großzügige Finanzierung des Projekts. Danken möchte ich auch den Mitgliedern der Arbeitsgruppe Sicherheit innerhalb des TA Elektronik im VDMA für die anregenden Diskussionen.

Widmen möchte ich diese Arbeit meiner Frau Susanne und unseren Kindern Lara und Benjamin. Danke für eure Unterstützung, eure Geduld und den Rückhalt, den ihr mir zuteil kommen lasst.

München, im Dezember 2004 Marcus Martinus

Geleitwort

Ähnlich wie bei Straßenfahrzeugen hat die Elektronik auch bei vielen mobilen Arbeitsmaschinen inzwischen große Bedeutung erlangt. Rasch zunehmende Automatisierungen gelten vor allem der Produktivitätserhöhung, der Ressourcenschonung und der Entlastung des Fahrers. Hierzu war an meinem früheren Lehrstuhl ein erstes, zunächst von der Industrie, dann auch von der DFG unterstütztes Projekt von Herrn Freimann bearbeitet worden, das der Automatisierung des Systems „Traktor und Gerät“ und dessen modellgestützter Entwicklung galt. Schon bei den damaligen Untersuchungen wurde deutlich, dass das Thema „Funktionale Sicherheit“ bei mechatronischen Systemen mobiler Arbeitsmaschinen große Bedeutung gewinnt, wie es ähnlich z. B. auch im Automobilbau der Fall ist.

Eine Vertiefung der Arbeiten in dieser Richtung wurde dann u. a. über die Mitarbeit in Arbeitskreisen des VDMA Fachverband Landtechnik angeregt. Herr Martinus übernahm diese Aufgabe und verantwortete das DFG-Projekt „Prozesssicherheit Landmaschinenelektronik“. Er schlägt nun mit seiner Dissertationsschrift einen Entwicklungsprozess mit zugeordneten Methoden und Werkzeugen vor, um bei mechatronischen Systemen mobiler Arbeitsmaschinen eine angemessene funktionale Sicherheit zu erreichen. Nach der systematischen Risiko-Abschätzung erfolgt die modellgestützte Entwicklung der Sicherheitstechnik. Die Grundlagen werden z. T. aus dem Automobilbau und anderen Bereichen abgeleitet und gezielt auf mobile Arbeitsmaschinen zugeschnitten.

Die Feldversuche mit provozierten Fehlern weisen aus, dass man mit systematischen, modellgestützten Auslegungen für mechatronische Systeme mobiler Arbeitsmaschinen einen ausreichend hohen Sicherheitsreifegrad erreichen kann, noch bevor das System überhaupt zum ersten Mal „in Stahl und Eisen“ zum Laufen gebracht wird.

Herr Dr.-Ing. M. Martinus entwickelte sich bereits frühzeitig zu einem kompetenten Fachmann für die funktionale Sicherheit mechatronischer Systeme. Meine Anerkennung und mein besonderer Dank gelten seiner weit überdurchschnittlichen Gesamtleistung, die er mit großer Selbständigkeit, Umsicht und Beharrlichkeit auf einem sehr neuen Gebiet erreichte.

Daneben danke ich allen beteiligten Mitarbeitern und Förderern – besonders der Deutschen Forschungsgemeinschaft (DFG) sowie den Firmen AGCO-Fendt und Lemken für ihre großzügige Unterstützung.

Garching, im Dezember 2004 Prof. Dr.-Ing. Dr. h.c. Karl Th. Renius

Inhaltsverzeichnis

Formelzeichen und Abkürzungen

Formelzeichen

α	%	Hubwinkel der Aufsattelkinematik
α	-	Durchflusskoeffizient
A	m^2	Querschnittsfläche der Blendenöffnung
α_1	%	Hubwinkel der Aufsattelkinematik, Sensor 1
A_1	m^2	Querschnitt der Blendenöffnung Verbraucher 1
α_2	%	Hubwinkel der Aufsattelkinematik, Sensor 2
A_2	m^2	Querschnitt der Blendenöffnung Verbraucher 2
$\alpha_{3_analytisch}$	%	Hubwinkel der Aufsattelkinematik, analytisch hergeleitet
$\alpha_{Referenz}$	%	Hubwinkel der Aufsattelkinematik, gültiger Referenzwert
A_{Ring}	m^2	Kolbenringfläche des Aufsattelzylinders
b	m	Arbeitsbreite
δ	°	Lenkwinkel
Δp_{LS}	bar, Pa	Druckdifferenz an der Blende (Differenzdruckregelung)
f	Hz	Frequenz
φ	°	Kurswinkel
l	m	Länge
m	kg	Masse
M	Nm	Drehmoment
M_{ZW_max}	Nm	maximal zulässiges Moment an der Zapfwelle
n	min^{-1}	Drehzahl
p	bar, Pa	Druck
p_1	bar, Pa	Druck am niederbelasteten Verbraucher
p_1'	bar, Pa	Druck vor der Druckwaage (Verbraucher 1)
p_2	bar, Pa	Druck am höherbelasteten Verbraucher
p_2'	bar, Pa	Druck vor der Druckwaage (Verbraucher 2)
Q	l/min, l/s	Durchfluss
Q_1	m^3/s	Durchfluss Verbraucher 1
Q_2	m^3/s	Durchfluss Verbraucher 2
Q_{V1}	l/min, l/s	Durchfluss Ventil 1 (Kreiseleggenaufsattelung)
Q_{V2}	l/min, l/s	Durchfluss Ventil 2 (Drillengebläse)
Q_{V3}	l/min, l/s	Durchfluss Ventil 3 (Spuranreißer)
Q_{V4}	l/min, l/s	Durchfluss Ventil 4 (Blindstrom Verstelldrossel)
ρ	kg/m^3	Dichte

r	%	Residuum des Aufsattelwinkels (normiert)
s_{Aushub}	m	Während des Aushubvorgangs zurückgelegte Strecke
$s_{Zielpunkt}$	m	Abstand Peilpunkt (Bearb.-grenze)–Gespannreferenzpunkt
t	s	Zeit
t_a	s	Auslösezeit der MSR-Sicherheitsfunktion
t_e	s	Fehlererkennungszeit der MSR-Sicherheitsfunktion
t_{Rest}	s	Zeit bis zum Treffpunkt Bearbeitungsgrenze/Arbeitspunkt
t_w	s	Zeit für Wirksamwerden der Sicherheitsmaßnahmen
U	V	Spannung
v	km/h, m/s	Geschwindigkeit
v_{ist}	km/h	Ist-Geschwindigkeit
v_{max}	km/h	maximal zulässige Geschwindigkeit
v_{max_Egge}	km/h	maximal zulässige Geschwindigkeit der Kreiselegge
v_{max_Packer}	km/h	maximal zulässige Geschwindigkeit des Ringpackers
v_{max_Task}	km/h	maximal zulässige Geschwindigkeit des Taskcontrollers
v_{soll}	km/h	Sollgeschwindigkeit
v_{soll_Egge}	km/h	Sollgeschwindigkeit der Kreiselegge
v_{soll_Packer}	km/h	Sollgeschwindigkeit des Ringpackers
V_{V1}	l	Volumen für Ventil 1 (Kreiseleggenaufsattelung)
x_R	m	x-Koordinate des Gespannreferenzpunktes
$x_{Versatz}$	m	seitlicher Versatz des Gespanns beim Wenden
y_R	m	y-Koordinate des Gespannreferenzpunktes
y_{Start}	m	y-Koordinate für automatischen Start des Einsetzvorgangs
z	m	Länge des Aufsattelzylinders

Abkürzungen

A	Auftretenswahrscheinlichkeit
A	Aufenthaltsdauer
ACC	Adaptive Cruise Control
AD/DA	Analog-Digital/Digital-Analog
AK	Anforderungsklasse
ASAE	American Society of Agricultural Engineers
B	Bedeutung
BA	Bremsassistent
BIOS	Basic Input Output System

BUS	Binary Unit System
CAN	Controller Area Network
Cat	Kategorie
CEN	Comité Européen de Normalisation
CMMI	Capability Maturity Model Integration
D	Diagnosemöglichkeit durch Selbstprüfung
DE	Dringend empfohlene Entwicklungsmethode oder -maßnahme
DFG	Deutsche Forschungsgemeinschaft
DGPS	Differential Global Positioning System
DIN	Deutsches Institut für Normung
DIS	Draft International Standard
E	Entdeckenswahrscheinlichkeit
E	Empfohlene Entwicklungsmethode oder -maßnahme
E/E/PES	elektrisch/elektronisch/programmierbar elektronische Systeme
ECE	Economic Commission for Europe
EE	Elektrik/Elektronik
EEPROM	Electrical Erasable Programmable Read Only Memory
EG	Europäische Gemeinschaft
EHR	Elektronisch-hydraulische Hubwerksregelung
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
ESP	Elektronisches Stabilitätsprogramm
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
FKH	Frontkraftheber
FMEA	Fehlermöglichkeits- und -einflussanalyse
G	Fahrzeugklasse: Geländefahrzeuge
G	Gefahrenabwendung
GPS	Global Positioning System
GUI	Graphical User Interface
HIL	Hardware-in-the-Loop
HKH	Heckkraftheber
HW	Hardware
HZW	Heckzapfwelle
I/O	In/Out
IEC	International Electrotechnical Commission

ISO	International Organization for Standardization
Kfz	Kraftfahrzeug
lof	land- oder forstwirtschaftlich
M, M1, ...	Fahrzeugklasse: Kraftfahrzeuge zur Personenbeförderung
MIL	Model-in-the-Loop
MISRA	Motor Industry Software Reliability Association
MSR	Messen, Steuern, Regeln
N, N1, ...	Fahrzeugklasse: Kraftfahrzeuge zur Güterbeförderung
NASA	National Aeronautics and Space Administration
Nkw	Nutzkraftwagen, Nutzfahrzeug
O, O1, ...	Fahrzeugklasse: Anhänger
OEM	Original Equipment Manufacturer
PC	Personal Computer
PIL	Processor-in-the-Loop
Pkw	Personenkraftwagen
PL	Performance Level
RCP	Rapid-Control-Prototyping
RPZ	Risikoprioritätszahl
RÜFA	Rückfahreinrichtung
S	Schadenausmaß
SAE	Society of Automotive Engineers
SCA	Software-Criticality-Analysis
SF	Sicherheitsfunktion
SIL	Software-in-the-Loop
SIL	Safety Integrity Level
SPICE	Software Process Improvement and Capability Determination
StVZO	Straßenverkehrs-Zulassungs-Ordnung
SW	Software
TMS	Traktor Management System
TR	Technical Report
TTCAN	Time Triggered CAN
TTP	Time Triggered Protocol
UKW	Ultrakurzwelle
UNECE	United Nations Economic Commission for Europe
URL	Uniform Resource Locator
V	Vornorm

VDA	Verband der Automobilindustrie
VDI	Verein Deutscher Ingenieure
VDMA	Verband Deutscher Maschinen- und Anlagenbau
V-Modell	Vorgehensmodell
W	Eintrittswahrscheinlichkeit
xooy	x out of y
ZW	Zapfwelle
PCMCIA	PC-Memory Card International Association
vo	vorne
hi	hinten
ret	retract
ext	extend
LUDV	Lastdruckunabhängige Durchflussverteilung

Kurzfassung – Abstract

Zukünftige mechatronische Systeme von mobilen Arbeitsmaschinen stellen spezielle Anforderungen an ihre funktionale Sicherheit. Diesbezüglich wurde ein sicherheitsgerichtetes Entwicklungskonzept aus Vorgehensmodell, Methoden und Werkzeugen erarbeitet, welches die notwendigen Maßnahmen von der Systemsynthese bis zur Validierung beschreibt. Als Versuchsträger diente eine typische Traktor/Geräte-Kombination, in der über den Stand der Technik hinausgehende Automatisierungsstrategien in Form eines vollständigen Vorgewendemanagements sowie der autonomen Prozessführung (Prinzip „Gerät steuert Traktor") realisiert wurden. Auf Grund von Parallelen in Systemaufbau, verwendeten Technologien und dynamischem Arbeitsumfeld steht die ausgewählte Anwendung beispielhaft für mobile Arbeitsmaschinen. In vorliegender Arbeit wird das Vorgehensmodell des Entwicklungskonzepts zunächst allgemein beschrieben. Geeignete, teilweise weiterentwickelte Methoden werden vorgestellt und aufbauend auf einer sicherheitsgerechten Systemarchitektur den einzelnen Entwicklungsschritten zugeordnet. Entscheidungskriterium ist dabei das geforderte maximale Risikoniveau für das betreffende System. Vorteile einer durchgängig modellbasierten Vorgehensweise werden aufgezeigt. Abschließend dokumentieren die Versuchsergebnisse die Validierung der nach dem Entwicklungskonzept erarbeiteten Automatiken des Versuchsträgers und erlauben die Verallgemeinerung der Ergebnisse auf den gesamten Bereich der mobilen Arbeitsmaschinen.

Future mechatronic systems of mobile working machinery have special requirements to satisfy functional safety. Therefore a safety-aligned development concept, consisting of process model, methods and tools, was worked out, which describes the required measures from synthesis to validation of mechatronic systems. A typical tractor/implement-combination was used as testing object, where automation strategies in terms of complete headland management or autonomous process-automation ("Implement Guided Tractor Control") above the state of the art were implemented. Due to parallels in system architecture, available technologies and dynamic working circumstances, the selected application is exemplary for mobile working machinery. This thesis describes generally the process model of the development concept. After choice of safety-appropriate system architecture suitable, partly enhanced methods are introduced and assigned to each development step. Therefore the specified maximum risk level for the corresponding system is decision criterion. Advantages of a continuous model-based approach are shown. Finally test results document validation of the experimental vehicle automatics, which had been worked out according the development concept, and allow generalization of the results for the whole area of mobile working machinery.

1 Einleitung und Aufgabenstellung

Die Entwicklungstendenzen bei mobilen Arbeitsmaschinen wurden in den letzten Jahren von einer überdurchschnittlichen Zunahme elektronisch gesteuerter und geregelter Prozesse bestimmt. Die Verschmelzung der Disziplinen Elektrotechnik, Informationstechnik und Maschinenbau zur Mechatronik wird zukünftig den größten Teil der Innovationen für sich einnehmen. Ein herausragendes Beispiel für den Wandel von der Mechanisierung zur Elektronifizierung als wichtigste Triebfeder zukünftiger Verbesserungen mobiler Arbeitsmaschinen ist das Segment der Landtechnik. Innovative Entwicklungstendenzen, wie teilflächenbezogene Applikation von Düngemitteln und Pflanzenschutz (Precision Farming [1]) oder Erhöhung der Schlagkraft durch (teil-)automatisierte Arbeitsprozesse in der Feldrobotik, werden die Mechanisierung als bisherigen Motor der Produktivitätssteigerung ablösen, vergleiche auch [2]. Neben der Produktivitätssteigerung stehen auch Verbesserungen der Arbeitsbedingungen für den Fahrer im Mittelpunkt der Bemühungen. Innovative Bedienkonzepte, elektromechanische bzw. -hydraulische Betätigungen, Unterstützung durch Teilautomatisierungen und elektronisch geregelte Arbeitsprozesse entlasten den Fahrer erheblich und sind mittlerweile Stand der Technik.

Ähnlich wie bei Traktoren und Landmaschinen sieht man auch bei Baumaschinen und in der Kommunaltechnik großes Innovationspotenzial im Einsatz mechatronischer Systeme und Automatiken. Hier liegt die Intention hauptsächlich in der Entlastung des Fahrers durch einfachere Betätigungskonzepte und Automatisierungen häufig verwendeter oder komplizierter Betätigungssequenzen. Die Arbeitsprozesse werden dadurch beschleunigt, eine Erhöhung der Schlagkraft und Reduzierung der Kosten wird möglich.

In Maschinen, wo noch keine zusätzlichen Funktionalitäten implementiert werden, schafft man derzeit die Voraussetzungen, zukünftigen Anforderungen des Wettbewerbs nachzukommen. Elektronische Regelung des Antriebsstrangs, systemübergreifende Datenkommunikation und elektronisch ansteuerbare Schnittstellen erweitern hier das Potenzial der Maschinensysteme für zukünftige Automatiken.

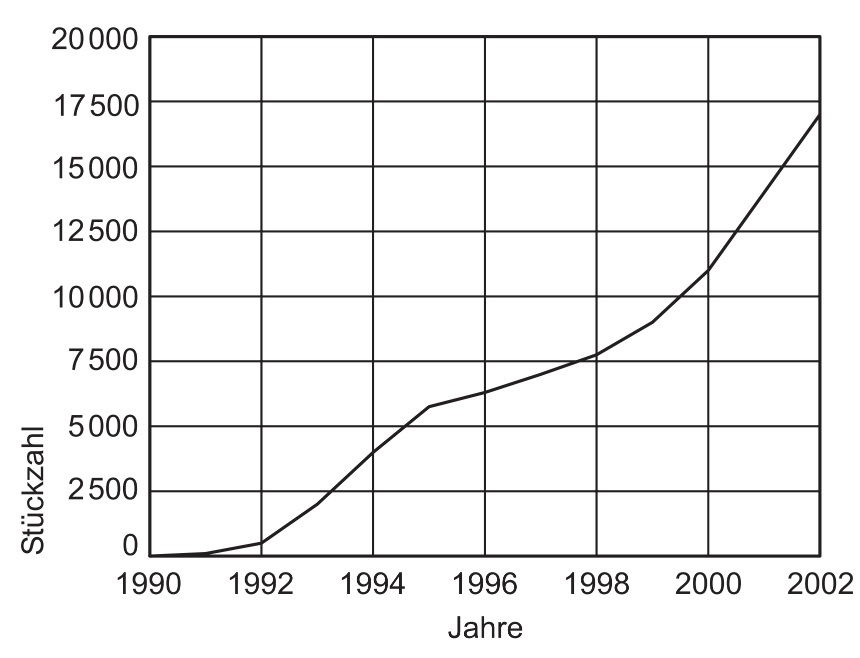


Bild 1-1: *Stückzahlentwicklung von elektronischen Steuergeräten mit CAN-Schnittstelle eines Herstellers[1)] [3].*

Ein Beispiel für den steigenden Anteil von Elektronik bei mobilen Arbeitsmaschinen zeigt die Darstellung in **Bild 1-1**. Hier ist die Stückzahlentwicklung für elektronische Steuergeräte mit CAN-Schnittstelle (Controller Area Network) eines renommierten Herstellers[1)] gezeigt. Der Absatz von elektronischen Steuergeräten für mobile Arbeitsmaschinen hat sich demnach in den letzten sieben Jahren verdreifacht.

1.1 Ausgangssituation und Problemstellung

Immer mehr Arbeitsprozesse mobiler Maschinensysteme sind durch automatisierte Vorgänge geprägt, in denen der Fahrer nur noch als übergeordnetes Kontrollorgan fungiert und die Funktionserfüllung den verschiedenen Automatiken überlassen kann. Sensor- und Aktoreinheiten sind hierbei nicht unbedingt zentral koordiniert, sondern möglicherweise über verteilte, gleichberechtigte Teilsysteme in die Regelung des systemübergreifenden Arbeitsprozesses eingebunden.

Dieser Trend stellt neue Anforderungen an die Betriebssicherheit, da bewährte mechanische Systeme durch innovative Mechatronik ersetzt werden und mechanische bzw. hydraulische Rückfallebenen in vielen Fällen wegfallen. Der Entwicklung dieser so genannten elektrisch/elektronisch/programmierbar elektronischen Systeme (E/E/PES) kommt hinsichtlich Erfüllung ihrer funktionalen Sicherheit eine besonders große Bedeutung zu. Im Moment sind weitestgehend noch keine speziell auf mobile Arbeitsmaschinen zugeschnittene Standards oder angepasste Produktnormen vorhanden. Um die Entwicklungsprozesse bei einem vernünftigen Aufwand/Nutzen-Verhältnis überschaubar und nachvollziehbar zu belassen, aber auch der geforderten funktionalen Sicherheit der Systeme nicht auf Kosten der Verfügbarkeit Rechnung zu tragen, sind neue spezifisch an die Entwicklung von mobilen Arbeitsmaschinen angepasste Vorgehensmodelle nötig.

---

1) Sensor-Technik Wiedemann GmbH, Kaufbeuren

Landmaschinen nehmen eine beispielhafte Stellung bezüglich ihrer universellen Einsatzspektren und Komplexität der maschinellen Arbeitsprozesse unter mobilen Arbeitsmaschinen ein. Am ehemaligen Lehrstuhl für Landmaschinen der Technischen Universität München wurde deshalb ein von der Deutschen Forschungsgemeinschaft (DFG) unterstütztes Projekt „Prozesssicherheit systemübergreifender Regelkreise und Automatiken im Betrieb von Traktor/Geräte-Kombinationen und selbstfahrenden Landmaschinen“ initiiert. Ziel war die Erarbeitung eines Entwicklungskonzepts, welches die funktionale Sicherheit dieser Systeme sichergestellt.

1.2 Vorgehensweise und Aufbau der Arbeit

Die vorliegende Arbeit stellt Entwicklungsschritte, Methoden und Werkzeuge des Entwicklungskonzepts für mechatronische Systeme bei mobilen Arbeitsmaschinen vor, befasst sich mit der Entwicklung eines konkreten Beispiels aus der Landtechnik und abstrahiert die Ergebnisse zu allgemeingültigen Regeln für die Anwendung bei mobilen Arbeitsmaschinen.

Zu Beginn der Arbeit (Kapitel 2) wird der aktuelle Stand der Technik beschrieben. Nach der Abgrenzung des thematischen Rahmens werden Beispiele von mechatronischen Systemen bei mobilen Arbeitsmaschinen vorgestellt und die zur Realisierung notwendigen Komponenten, Technologien und Entwicklungsprozesse behandelt. Aktuelle Standards, Normungsprojekte und relevante Richtlinien, die für eine sicherheitsgerechte Entwicklung als Grundlage dienen können, runden diesen Abschnitt ab.

Das Kapitel 3 ist den theoretischen Grundlagen der Sicherheitstechnik für die Gewährleistung des sicheren Zustands gewidmet. Die funktionale Sicherheit wird als Bestandteil der konstruktiven Sicherheit definiert und es werden Anforderungen bezüglich zulässiger Risiken der mechatronischen Systeme bei mobilen Arbeitsmaschinen aufgestellt.

Der darauf folgende Teil der Arbeit konzentriert sich auf empfohlene, verwendete und weiterentwickelte Entwicklungsmethoden (Kapitel 4) und ihre Anordnung im erarbeiteten Entwicklungskonzept (Kapitel 5). Abhängig vom Risikopotenzial der Systeme werden sicherheitsgerechte Systemarchitekturen vorgeschlagen und geeignete Methoden den Entwicklungsschritten zugeordnet. Der Vorteil einer durchgängig modellbasierten Vorgehensweise wird dabei deutlich gemacht.

Die Vorgehensweise sollte anhand eines Anwendungsbeispiels verifiziert und weiterentwickelt werden. Im Kapitel 6 wird der Versuchsträger und die sicherheitsgerechte Entwicklung seiner Automatiken beschrieben. Kapitel 7 behandelt die Versuchsdurchführung und Validierung des Gesamtsystems und verallgemeinert die Ergebnisse auf den gesamten Bereich der mobilen Arbeitsmaschinen.

2 Stand der Forschung und Technik

Die Beschreibung des Stands der Technik gliedert sich in vier Themengebiete. Zu Beginn werden maßgebliche Eigenschaften von mobilen Arbeitsmaschinen beschrieben und es wird ihr Entwicklungsstand bezüglich mechatronisch gestalteter Arbeitsprozesse beleuchtet. Schwerpunktmäßig werden ausgeführte Beispiele bei Landmaschinen vorgestellt, da sie eine exponierte und beispielhafte Stellung für mobile Arbeitsmaschinen einnehmen. Um Anregungen aus dem Bereich der Kraftfahrzeuge nutzen zu können, werden aktuelle übertragbare Entwicklungsprozesse und -konzepte für sicherheitskritische Systeme bei Kfz vorgestellt. Auch wenn der Anteil von spezifisch an mobile Arbeitsmaschinen angepasste Normen noch gering ist, gibt es doch technologieübergreifende Grundlagennormen und einzelne Anwender-Standards, die sich der funktionalen Sicherheit widmen und für mehrere Technologiezweige den Stand der Technik wiederspiegeln. Aktuelle Normen und Normungsprojekte, die sich um Bereiche funktionaler Sicherheit bemühen, werden zum Ende des Kapitels vorgestellt.

2.1 Definition der mobilen Arbeitsmaschine

Die unterschiedlichen Interpretationen von Zuordnungen mobiler Maschinentechnik zum Bereich mobiler Arbeitsmaschinen lassen keine einheitliche Definition für mobile Arbeitsmaschinen erkennen. Meistens werden unterschiedliche Bereiche des Maschinenbaus wie Baumaschinen, Fördermaschinen und Landmaschinen zum Bereich mobile Arbeitsmaschinen zusammengefasst [4]. Damit werden aber auch quasistationär arbeitende Maschinen, die im eigentlichen Sinne nicht dazu zählen, mit eingeschlossen, z. B. Melkroboter, Baukräne, Seilbahnen, etc.. Weiter gegriffene Ansätze schließen außerdem die Bereiche Kommunalmaschinen, Forstmaschinen sowie Spezialmaschinen (Feuerwehr, Pistenraupen oder Militärtechnik) mit ein, distanzieren sich aber von der Fahrzeugtechnik im Sinne von Land-, Wasser- und Luftfahrzeugen [5, 6]. Ein anderer Ansatz ist die Klassifizierung mobiler Arbeitsmaschinen nach ihrer Abgeschlossenheit [7]. **Abgeschlossene** Maschinensysteme sind ab Werk vollständig konfiguriert, programmiert und damit sofort

einsetzbar, z. B. Radlader. Im Gegensatz dazu haben **kombinierte** Maschinensysteme, z. B. Traktoren, offene Schnittstellen hinsichtlich Mechanik, Hydraulik, Elektrik oder Elektronik und sind zur Arbeitserledigung in der Regel auf externe Geräte angewiesen.

In den internationalen produktspezifischen Normen und Richtlinien (z. B. bezüglich Typgenehmigung oder Betriebserlaubnisverfahren) finden sich zwar mögliche Ansätze zur Klassifizierung mobiler Arbeitsmaschinen, die nicht direkt spezifizierten Teilsegmente anderer Maschinensysteme sind aber meistens aus dem Geltungsbereich ausgeschlossen. Nach der EG-Richtlinie 70/156/EWG [8] werden Fahrzeuge mit mindestens vier Rädern in die Klassen M (Kraftfahrzeuge zur Personenbeförderung), N (Kraftfahrzeuge zur Güterbeförderung), O (Anhänger) eingeteilt, die mit der Option G für Geländefahrzeuge kombiniert werden können, dargestellt in **Tabelle 2-1**.

Tabelle 2-1: *Fahrzeugklassen nach EG-Richtlinie 70/156/EWG [8]*

<table>
<tr><th colspan="3">Kraftfahrzeuge mit mindestens vier Rädern und Anhänger</th></tr>
<tr><th>Klasse M: Kraftfahrzeuge zur Personenbeförderung</th><th>Klasse N: Kraftfahrzeuge zur Güterbeförderung</th><th>Klasse O: Anhänger (einschließlich Sattelanhänger)</th></tr>
<tr><td>M1: höchstens acht Sitze außer dem Fahrersitz</td><td>N1: zulässige Gesamtmasse von bis zu 3,5 t</td><td>O1: zulässige Gesamtmasse von bis zu 0,75 t</td></tr>
<tr><td>M2: mehr als acht Sitze außer dem Fahrersitz und zulässige Gesamtmasse bis zu 5 t</td><td>N2: zulässige Gesamtmasse von mehr als 3,5 t bis zu 12 t</td><td>O2: zulässige Gesamtmasse von mehr als 0,75 t bis zu 3,5 t</td></tr>
<tr><td>M3: mehr als acht Sitze außer dem Fahrersitz und zulässige Gesamtmasse von mehr als 5 t</td><td>N3: zulässige Gesamtmasse von mehr als 12 t</td><td>O3: zulässige Gesamtmasse von mehr als 3,5 t bis zu 10 t</td></tr>
<tr><td colspan="2">Symbol G: Geländefahrzeuge</td><td rowspan="2">O4: zulässige Gesamtmasse von mehr als 10 t</td></tr>
<tr><td colspan="2">Fahrzeuge der Klassen M und N, die für den Einsatz abseits der Straße bestimmt sind, können zusätzlich mit dem Symbol G gekennzeichnet werden.[a)]</td></tr>
</table>

a) Die Bezeichnung eines geländegängigen Fahrzeugs zur Güterbeförderung mit 5 t Gesamtmasse lautet dann z. B. N2G.

Mobile Arbeitsmaschinen könnten nach dieser Definition in die Klassen N1G bis N3G eingeteilt werden, sind aber aus dem Geltungsbereich dieser Richtlinie ausdrücklich ausgenommen. Die eigentlichen Vertreter der in dieser Arbeit behandelten mobilen Arbeitsmaschinen findet man in spezifisch angepassten Produktnormen bzw. Richtlinien für Baumaschinen, Land- oder Forstmaschinen (lof-Maschinen) und selbstfahrende Arbeitsmaschinen, siehe **Tabelle 2-2**.

***Tabelle 2-2:** Produktspezifische Normen als Definitionsgrundlage für mobile Arbeitsmaschinen.*

Land- und Forstmaschinen	EG-Richtlinie 2003/37/EG [9]
Baumaschinen	DIN EN ISO 6165/A1 [10, 11]
Mobile Maschinen	EG-Richtlinie 97/68/EG [12]

Die EG-Richtlinie 2003/37/EG [9] bezieht sich auf Zugmaschinen, Anhänger und gezogene auswechselbare Maschinen für den Einsatz in der Land- oder Forstwirtschaft, schließt aber Erdbaumaschinen, definiert nach ISO 6165 [10, 11], ausdrücklich aus. Auch die EG-Richtlinie 97/68/EG [12] für Maßnahmen zur Bekämpfung von Schadstoffemissionen bei mobilen Maschinen kommt für eine Definition mobiler Arbeitsmaschinen nicht in Betracht. Sie fasst zwar Baumaschinen, bestimmte Fördermaschinen und Spezialmaschinen zu einem Bereich „Arbeitsmaschinen" zusammen, isoliert aber wiederum Land- und Forstmaschinen. Ein Grundlagenpapier, um den Bereich der mobilen Arbeitsmaschinen festzusetzen, fehlt damit.

In der vorliegenden Arbeit werden somit mobile Arbeitsmaschinen als Maschinen mit folgenden Kriterien definiert:

- Die **Erledigung eines Arbeitsprozesses** steht im Vordergrund ihrer Funktionalität.
- Die **eigenständige Fortbewegung** ist direkte Voraussetzung ihrer Hauptfunktion(en), entweder als Teilprozess der Hauptfunktionalität (z. B. Vorschub eines Straßenfertigers) oder als Nebenfunktion (z. B. Traktor mit Güllepumpe: stationärer Betrieb mit Möglichkeit zur Transportfahrt).
- Die Mobilität der Maschine darf nicht an festgelegte Bahnen, wie z. B. Schienensysteme, Induktionsschleifen, etc., gebunden sein, d. h. das **Arbeitsumfeld** der Maschine ist **dynamisch veränderbar** und **frei wählbar**. Es unterliegt in der Regel wechselnden Umwelteinflüssen.

Aus dieser Definition ergeben sich verschiedene Konsequenzen bzw. Merkmale:

- Da eine **stationäre Energieversorgung** schwer zu realisieren ist, wird die benötigte Energie grundsätzlich aus Speichern bezogen. Energieverbrauch, Leistungsgewicht, etc. werden deshalb zu wichtigen Kenngrößen.
- Durch das dynamische Einsatzumfeld muss auf **Umweltverträglichkeit** hinsichtlich Schadstoffausstoß, Elektromagnetischer Verträglichkeit (EMV), etc. besonders Wert gelegt werden.
- Das wechselnde Arbeitsumfeld stellt besondere Anforderungen an die **Betriebssicherheit** hinsichtlich Bedienpersonen und Unbeteiligten. Spezielle Maßnahmen sind bei Teilnahme am öffentlichen Straßenverkehr zu erfüllen (z. B. Erfüllung der StVZO [13] bei Transportfahrten).

- Die Einteilung in Leistungsklassen kann auf mehreren Ebenen geschehen. Für Spezifikationszwecke ergeben sich somit **verschiedene Leistungskennzahlen** z. B. für Fahrleistung, Hubleistung, Förderleistung, Durchsatz, etc..
- Eine Unterteilung mobiler Arbeitsmaschinen in **abgeschlossene Maschinensysteme** mit und ohne Werkzeugwechsel und **kombinierbare Maschinensysteme** mit offenen Schnittstellen ist sinnvoll, siehe auch [7].

Basierend auf dieser Definition wird in vorliegender Arbeit das Themengebiet der mobilen Arbeitsmaschinen abgesteckt. **Tabelle 2-3** zeigt Beispiele mobiler Arbeitsmaschinen und die dazugehörigen Obermengen (Maschinenklassen), siehe auch [14-17].

Tabelle 2-3: *Beispiele für mobile Arbeitsmaschinen mit Obermengen.*

Mobile Arbeitsmaschinen aus den Bereichen					
Bau-maschinen	**Land-maschinen**	**Forst-maschinen**	**Kommunal-maschinen**	**Förder-maschinen**	**Sonstige Spezialmaschinen**
• Lademaschinen • Bagger • Planiermaschinen • Walzen • Straßenfertiger • ...	• Traktoren • Traktor/Geräte-Kombinationen • Vollerntemaschinen • Geräteträger • Feldhäcksler • ...	• Forstschlepper • Harvester • mobile Sägewerke • ...	• Winterdienste • Reinigungsmaschinen • Universalmäher • ...	• Lademaschinen • Autokräne • Stapler • Muldenkipper • Betonpumpen • ...	• Militärfahrzeuge • Feuerwehr • Pistenraupen • Strandreiniger • ...

Einige Beispiele von mobilen Arbeitsmaschinen können definitionsgemäß mehreren Bereichen zugeordnet werden, wie z. B. der Radlader als Teilmenge der Baumaschinen wie auch der Fördermaschinen.

2.2 Mechatronische Systeme bei mobilen Arbeitsmaschinen

Wie in [18] beschrieben, wurde der Begriff „Mechatronics" (zu Deutsch Mechatronik) im Jahre 1969 vom Japaner Ko Kikuchi, Präsident der YASKAWA Electronic Corporation, geprägt. Der Hersteller automatisierungstechnischer Produkte, wie Servoantriebe und Roboter, verstand darunter die elektronische Funktionserweiterung mechanischer Komponenten. Der Begriff setzt sich zusammen aus Mechanism (später Mechanics, Mechanik oder allgemeiner Maschinenbau) und Electronics (Elektronik oder allgemeine Elektrotechnik) und war im Zeitraum 1971 bis 1982 als Handelsname geschützt [19]. Isermann konkretisiert den Begriff und beschreibt Mechatronik als interdisziplinäres Gebiet, bei dem die Disziplinen Maschinenbau, Elektrotechnik und Informationstechnik zusammen-

wirken [20], wie es auch in **Bild 2-1** gezeigt ist. Die Synergien der Zusammenführungsprozesse stehen dabei im Vordergrund.

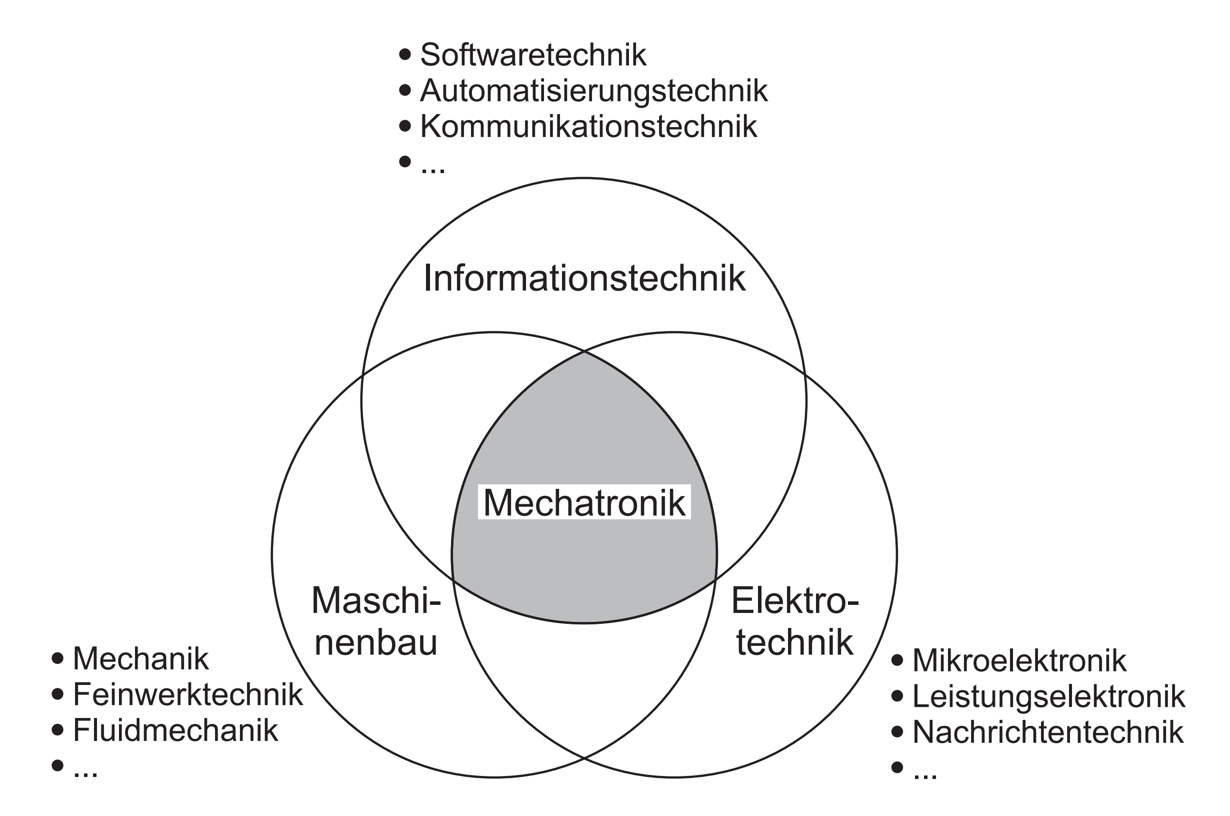


Bild 2-1: *Mechatronik – Synergie aus dem Zusammenwirken verschiedener Disziplinen mit Beispielen für unterschiedliche Technologiebereiche, vergleiche [20].*

In vorliegender Arbeit wird die Definition mechatronischer Systeme des Richtlinienentwurfes VDI 2206 [21] verwendet, die von Harashima, Tomizuka und Fukuda stammt [18]: “Mechatronics is the synergetic integration of mechanical engineering with electronic and intelligent computer control in the design and manufacturing of industrial products and processes.” 1)

Mechatronische Systeme bestehen demnach aus diskreten mechanischen und elektronischen Komponenten in Symbiose mit der Informationstechnik. Dabei sind unterschiedliche Ausprägungen mechatronischer Systeme bezüglich funktionaler und/oder räumlicher Integration denkbar – vom einfachen Ersatz mechanischer Funktionselemente durch elektronische Komponenten bis hin zum kompletten Neuentwurf auf der Basis eines mechatronischen Entwicklungsprozesses. Generell können mechatronische Systeme auch aus Subsystemen bestehen, die selbst wieder mechatronische Systeme sind [21]. In **Bild 2-2** ist die Strukturanalyse für den allgemeinen Aufbau mechatronischer Systeme gezeigt. Die

1) Freie Übersetzung: Mechatronik bezeichnet das synergetische Zusammenwirken der Fachdisziplinen Maschinenbau, Elektrotechnik und Informationstechnik beim Entwurf und der Herstellung industrieller Erzeugnisse sowie bei der Prozessgestaltung.

unterschiedlichen Elemente sind in der Black-Box-Darstellung durch die Umsatzarten Energie-, Stoff- und Information miteinander verbunden.

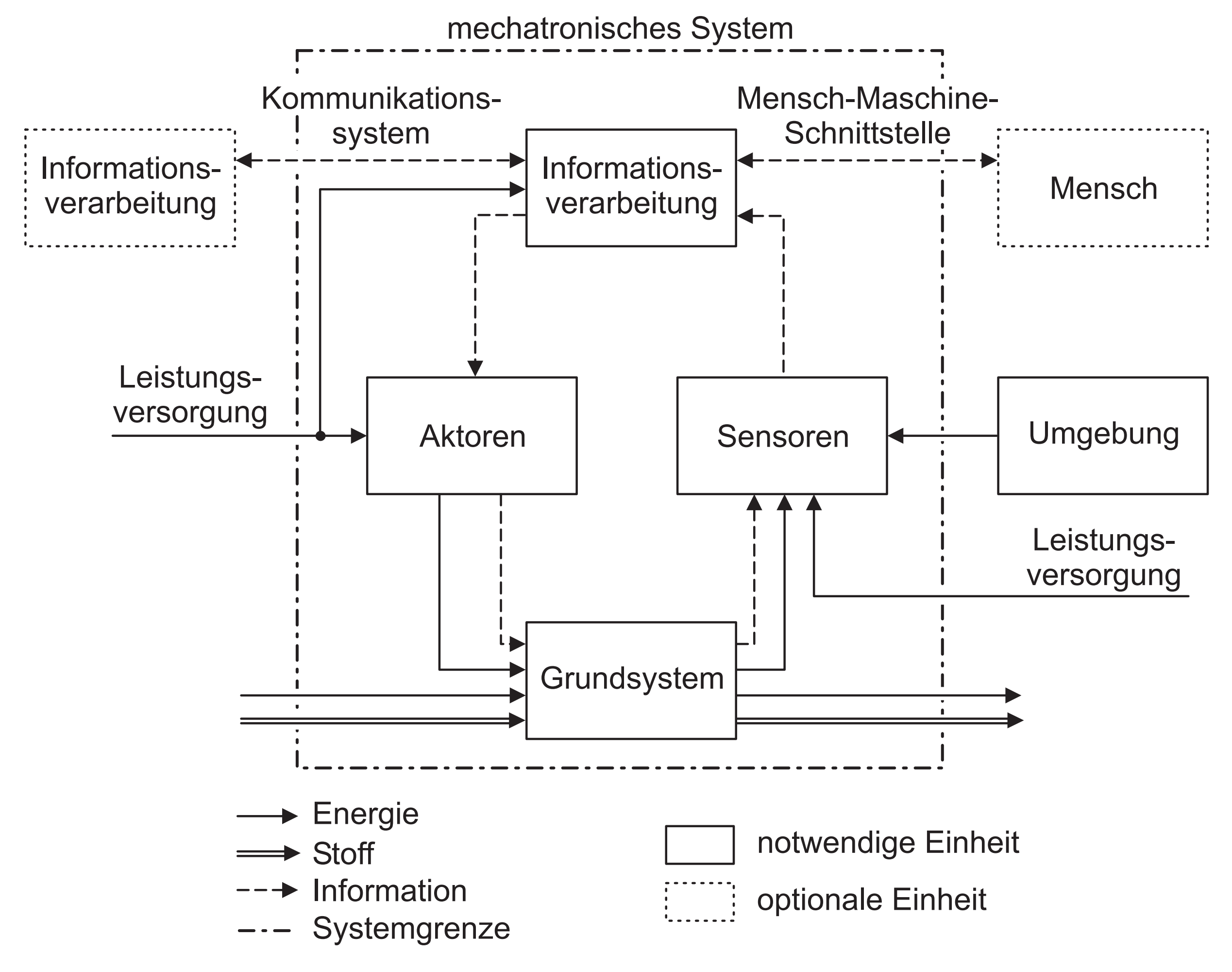


Bild 2-2: *Analyse der Grundstruktur eines mechatronischen Systems, vergleiche [21].*

Jedes mechatronische System besteht aus einem Grundsystem, Sensoren, Aktoren und einer Informationsverarbeitung. Das **Grundsystem** ist technologieunabhängig, d. h. es kann beispielsweise aus einer mechanischen, elektromechanischen, hydraulischen oder pneumatischen Struktur bestehen, bzw. auch aus Mischformen. Das Grundsystem ist über Energie- und Stoffflüsse über die Systemgrenzen hinaus mit anderen Systemen (z. B. der Umgebung), anderen mechatronischen (Teil-)Systemen oder auch anderen Grundsystemen verbunden. Die **Sensoren** ermitteln die notwendigen Zustandsgrößen des Grundsystems oder der Umgebung, in der das System betrieben wird. Sie können als konventionelle Messwertaufnehmer physisch real vorhanden sein oder durch analytische Software-Sensoren, so genannte „Beobachter", implementiert werden. Die **Informationsverarbeitung** (hardwareunabhängige Logik) bestimmt die notwendigen Aktionen, die nötig sind, um die Zustandsgrößen hinsichtlich Spezifikation des mechatronischen Systems zu beeinflussen. Optional ist sie zum Datenaustausch über ein Kommunikationssystem mit anderen logischen Einheiten verbunden. Über eine Mensch-Maschine-Schnittstelle kann dem Benutzer

die Möglichkeit zum Informationsaustausch gegeben werden, wodurch die Interaktion zwischen Mensch und mechatronischem System realisiert wird. Die Umsetzungen der von der Informationsverarbeitung bestimmten Aktionen erfolgt durch die **Aktoren** direkt am Grundsystem. Die Leistungsversorgung der Systemelemente kann über die Systemgrenzen hinaus durch externe Energiequellen, wie im Bild 2-2 dargestellt, oder auch intern durch das Grundsystem erfolgen.

Nach der allgemeinen Beschreibung mechatronischer Systeme soll in den nächsten Unterpunkten der diesbezügliche Stand der Entwicklungen bei mobilen Arbeitsmaschinen aufgezeigt werden. Unter anderem wurde in der ersten ASAE Konferenz „Automation Technology for Off-road Equipment“ in Chicago [22] deutlich, wie facettenreich die Automatisierungsmöglichkeiten mobiler Maschinensysteme sind.

2.2.1 Elektronischer Eingriff in die Fahrzeugführung

Gerade bei den Entwicklungen zur Fahrzeugführung von mobilen Arbeitsmaschinen kann von den Systemen bei Nutzfahrzeugen (Nkw) und Pkw profitiert werden. In Zukunft wird sich dieser Trend noch verstärken, da die Transportgeschwindigkeiten mobiler Arbeitsmaschinen auch weiterhin steigen und so mehr Parallelen und Synergiemöglichkeiten entstehen werden. Bei höheren Endgeschwindigkeiten werden die aus dem Automotive-Bereich bekannten Fahrerassistenzsysteme, auch unter Verwendung von X-by-Wire-Systemen, zur Entlastung des Fahrers und Verbesserung der aktiven Sicherheit mehr und mehr Einzug halten, Beispiele für Systeme bei Pkw und Nkw siehe [23-26], Grundlagen in [27, 28]. Damit begibt man sich aber auch auf Gebiete, wo die Zuverlässigkeit und vor allem die funktionale Sicherheit gesamter Systeme immer wichtiger werden. Die Entwicklungsprozesse und -methoden wie auch das Layout der Systeme müssen an die sicherheitskritischen Anwendungsfälle angepasst werden, besonders wenn auf Grund höherer Geschwindigkeiten neue Zulassungsrichtlinien greifen. Beispiel hierzu ist die hydraulische Einkreislenkung, die durch die StVZO in Fahrzeugen bis 50 km/h zugelassen wird und bei mobilen Arbeitsmaschinen weite Verbreitung findet. Eine Erhöhung der Zulassungsvorschriften auf 60 km/h ist in Vorbereitung, siehe Kapitel 2.4.

Profitierend von den Entwicklungen innovativer Fahrzeugführungssysteme bei Pkw und Nkw werden auch bei mobilen Arbeitsmaschinen die Systeme für Antriebsstrang und Lenkung von einem immer größer werdenden Teil an Elektronik bestimmt [29, 4]. Anwendungen im Automotive-Bereich sind hauptsächlich Fahrerassistenzsysteme, die den Fahrer bei Routineaufgaben entlasten, wie z. B. Adaptive Cruise Control[1)] (ACC),

1) Konventionelle Tempomatfunktion wobei zusätzlich der maximal gültige Abstand zum vorausfahrenden Fahrzeug durch Motormanagement und aktiven Bremseingriff eingeregelt werden kann [23].

oder Systeme der aktiven Sicherheit, die versuchen, Fahrstabilität oder Precrash-Eigenschaften des Fahrzeugs zu verbessern, z. B. Bremsassistent[1)] (BA). Ein zweiter Aspekt, der bei aktuellen Systemarchitekturen festgestellt werden kann, betrifft das Umdenken bezüglich der Signalübertragung zwischen Sensor und Aktor. Wird das Kraftsignal konventioneller Sensor/Aktor-Einheiten direkt mechanisch oder hydraulisch bzw. mit mechanischer oder hydraulischer Rückfallebene übertragen, so trennen moderne X-by-Wire-Systeme diese Verbindung auf und ersetzen sie durch diskrete oder digitale elektronische Signale, meist ohne mechanische oder hydraulische Rückfallebene. Um die Signale zu wandeln, müssen intelligente Sensoren und Aktoren mit integrierter Elektronik verwendet werden. Der Energiefluss zwischen Sensor und Aktor des konventionellen Systems wird somit durch einen logischen Informationsfluss ersetzt. Betrachtet man beispielsweise ein Brake-by-Wire-System, so wird die mechanisch/hydraulische Kraftübertragung zwischen Bremspedal und Bremsaktorik, also die Wirkkette Bremskraftverstärker, Leitungssystem und Bremszylinder, durch eine elektronische Signalübertragung zwischen Pedal und Aktor ausgetauscht.

Elektronischer Eingriff in Motor und Getriebe

Durch den anhaltenden Trend zu elektronisch geregelten Dieselmotoren und stufenlosen Getrieben bei Traktoren [31] wurden intelligente Managementsysteme für den Antriebsstrang möglich, die einerseits verbrauchsoptimierte, andererseits leistungsoptimierte Betriebsbereiche bei den unterschiedlichsten Einsatzfällen zur Verfügung stellen [32, 33]. In Weiterführung dieser Forschungsarbeiten werden die Ergebnisse auch auf andere mobile Arbeitsmaschinen wie z. B. Hydraulikbagger übertragen [34]. Durch Verheiratung intelligenter Antriebsstrangkonzepte mit neuen Möglichkeiten bei der Gestaltung der Mensch-Maschine-Schnittstelle kann der Fahrer unterschiedliche Betätigungskonzepte und Fahrstrategien flexibel bestimmen und miteinander kombinieren [35, 36]. Um automatische Managementfunktionen zu ermöglichen, setzt die Firma John Deere bei den Traktoren der 6000er und 7000er Baureihe auf stufenlose hydrostatisch-leistungsverzweigte Getriebe mit über CAN vernetzten elektronischen Steuereinheiten für Motor, Getriebe und Fahrerschnittstelle [37, 38]. AGCO-Fendt realisierte mit ihrem „Traktor Management System“ (TMS) vier unterschiedliche Betätigungsstrategien, die zwischen Fahrpedal- und Fahrhebelbetrieb jeweils mit und ohne Getriebe-Motormanagement unterscheiden [39, 40].

Weitere Konzepte verfolgen die Strategie automatisierter Vorgänge bei Lastschaltgetrieben mit ebenfalls elektronisch geregelten Motoren. Automatisches Anheben der Dreh-

1) Aus der Betätigungsgeschwindigkeit des Bremspedals erkennt der BA die Notwendigkeit einer Vollbremsung und stellt im Bremskraftverstärker vollen Bremsdruck bereit [30].

zahl (Power-by-Wire) beim Zurückschalten und Absenken der Drehzahl beim Hochschalten der Lastschaltstufe schont Fahrer und Getriebe durch einen lastunabhängig sanften Schaltvorgang im John Deere 6020er Traktor [41]. Automatisierte Schaltvorgänge der Lastschaltstufen (Shift-by-Wire) wurden von den Firmen Deutz-Fahr und ZF Friedrichshafen AG realisiert [42, 43].

Elektronischer Eingriff in die Betriebsbremse

Die Einsatzfälle von mobilen Arbeitsmaschinen bieten noch nicht das standardmäßige Umfeld, um die Vorteile von elektronisch betätigten Bremskonzepten, so genannten Brake-by-Wire-Systemen, zu nützen. Hauptsächlich werden diese Systeme bei Nutzfahrzeugen und Pkw mit höheren Endgeschwindigkeiten angewendet, wo selektive, automatische Bremseingriffe die aktive Sicherheit der Fahrzeuge verbessern können, z. B. elektronisches Stabilitätsprogramm ESP. Steigen in Zukunft die Transportgeschwindigkeiten mobiler Arbeitsmaschinen weiter an, werden sich auch hier Anwendungsmöglichkeiten mit elektrohydraulischem oder -mechanischem Bremseingriff bieten.

Ausnahmen dazu sind bei der Feldarbeit autonom navigierende Traktor/Geräte-Kombinationen mit elektrohydraulischem Bremseingriff, wie sie später beschrieben werden. Ein Forschungsprojekt der TU Braunschweig beschäftigt sich mit Grundlagen eines Bremsmanagements von Traktoren. Kritische Fahrzustände von Traktor/Anhänger-Kombinationen werden sensiert, um daraufhin das Gespann durch automatisch gezielte Bremseingriffe zu stabilisieren [44].

Elektronischer Eingriff in die Lenkung

Die zukünftigen Bestrebungen für Lenksysteme bei Nkw und Pkw beziehen sich auf neuartige Betätigungskonzepte, automatische Lenkeingriffe, dynamische Veränderung der Lenkübersetzung oder Designvorteile durch Reduzierung des Platzbedarfs des Lenksystems im Gesamtfahrzeugkonzept. Um sich diese Vorteile zu Nutze zu machen, ist grundsätzlich das Aufbrechen der mechanischen bzw. hydraulischen festen Verbindung zwischen Betätigungseinheit und lenkbarer Achse (Steer-by-Wire) erforderlich. Nach Pandit legt Steer-by-Wire damit den Grundstein für die Implementierung neuartiger Fahrerassistenzsysteme und Komfortfunktionen [45]. Auch bei mobilen Arbeitsmaschinen werden diese Ziele verfolgt. Zusätzlich dazu ergeben sich hier Möglichkeiten, durch intelligente Lenksysteme in den Arbeitsprozess direkt einzugreifen. Die Entwicklungen bei Lenksystemen können demnach eingeteilt werden in

- Erweiterungen der Komfortfunktionen, z. B. durch leichtgängige Potentiometerlenkungen und eine daraus resultierende hohe und/oder anpassbare Lenkübersetzung

und

- vollständig automatisierte Lenksysteme, wie automatisches Lenken von Landmaschinen bei der Feldarbeit.

Für die aktuellen Entwicklungen von zusätzlichen **Komfortfunktionen** gibt [46] einen Überblick zu elektromechanischen und -hydraulischen Lenksystemen für die Beeinflussung von Lenkwinkel bzw. Lenkmoment. Ein Beispiel aus dem Pkw-Bereich ist das Aktivlenkungssystem von BMW, welches die wesentlichen Steer-by-Wire-Funktionen bereitstellt, ohne auf den mechanischen Durchgriff zu verzichten [47, 48]. Bei dem System wurde ein Planetengetriebe als Überlagerungsgetriebe in die Lenksäule integriert. Je nach Fahrsituation werden zusätzliche Lenkwinkel (negativ oder positiv) an der Vorderachse automatisch erzeugt oder unterschiedliche Lenkübersetzungen geschwindigkeitsabhängig eingestellt. Bei Traktoren realisiert New Holland elektrohydraulisch ebenfalls zwei unterschiedliche Lenkübersetzungen, aber ohne mechanische Rückfallebene. Auf Knopfdruck kann von Normalbetrieb in einen Schnelleinschlagmodus zur Unterstützung von Frontladerarbeiten und des Wendens am Vorgewende umgeschaltet werden [41, 49]. Aus Sicherheitsgründen wird dieses System bei Geschwindigkeiten über 10 km/h abgeschaltet.

Bei speziellen Traktoren oder Baumaschinen ist es möglich, durch Rückfahreinrichtungen (RÜFA) den Fahrerplatz entgegen der eigentlichen Fahrtrichtung zu drehen und damit die Hauptarbeitsrichtung rückwärts in den Schubbetrieb umzukehren. Bei der Lösung für Fendt Traktoren werden die Lenksignale durch ein kleines Potentiometer in der Armlehne erzeugt und an eine elektronisch gesteuerte Ventileinheit übertragen [50, 51]. Das konventionelle Lenkrad wird im RÜFA-Betrieb nicht mitgeschwenkt. Bei Baumaschinen, wie z. B. Baggerladern, sind Wendeeinrichtungen für Fahrersitz und hydraulische Betätigungselemente in der Kabine, ähnlich der RÜFA bei Traktoren, schon seit längerem verbreitet. In den Kommunalfahrzeugen Unimog U 300, U 400 und U 500 gibt es optionale, mechanisch realisierte Wechsellenksysteme mit zwei arretierbaren Positionen für Lenkung und Pedallerie links und rechts, um die Position des Fahrerplatzes an die verschiedenen Arbeitseinsätze anzupassen, siehe [52]. Mittlerweile erhielt ein Unimog-Versuchsfahrzeug mit einem rein **elektronisch** realisierten System gleicher Funktionalität erstmals die Straßenzulassung für Nutzfahrzeuge1) als Beispiel für ein vollständig implementiertes Steer-by-Wire, siehe auch [25, 54].

Erweitert man die Lenkbarkeit mobiler Arbeitsmaschinen mit elektronischer Eingriffsmöglichkeit auf weitere Achsen des Fahrzeugs, ergeben sich neue Funktionsmöglichkeiten für Wendigkeit oder Bodenschonung. Beispiele hierfür sind schwere selbstfahrende Arbeitsmaschinen, die im so genannten Hundegang eine homogenere und damit in den

1) Eine Genehmigung für Pkw ist laut Kraftfahrt-Bundesamt wegen der weitaus höheren Geschwindigkeit nicht absehbar [53].

oberen Schichten geringere Bodenverdichtung erreichen [55] oder kleine wendige Traktoren mit Allradlenkung für den Einsatz im steilen Gelände, die elektrohydraulisch auf Betrieb mit Front-, Heck- und Hundeganglenkung umgeschaltet werden können, z. B. Mounty 65 von Reformwerke [56]. Im Baumaschinenbereich gibt es neue Ansätze, Mobilkräne durch Allradlenkung und Hundegangmöglichkeit für den Offroad-Einsatz auszurüsten [57].

Auch wenn Zulieferer schon Komplettlösungen für Steer-by-Wire-Systeme anbieten [58, 59] und Ausnahmelösungen (siehe Versuchsfahrzeug Unimog) die Zulassung erhalten haben, sind offiziell alle Lenksysteme für Fahrzeuggeschwindigkeiten größer 50 km/h, bei denen die feste Verbindung zwischen Lenkrad und Lenkaktorik durch elektronische Signalübertragung ersetzt wurde, noch nicht für den öffentlichen Straßenverkehr zugelassen. Bestrebungen, die gesetzlichen Regelungen für den Gang des Fortschritts anzupassen, sind im Kapitel 2.4 beschrieben.

Werden die Lenksignale nicht vom Fahrer, sondern von anderen auch externen Regeleinheiten erzeugt und über einen Steuerrechner dem Lenksystem zugeführt, spricht man von **automatischen Lenksystemen**, wobei man die Navigation nach realen und virtuellen Leitlinien unterscheidet [60]. In der Landwirtschaft gibt es einige Beispiele für die Navigation nach realen Leitlinien. **Tabelle 2-4** zeigt eine Auswahl geeigneter Sensorik, die auch bei Baumaschinen oder in der Kommunaltechnik ähnlich Anwendung findet.

Tabelle 2-4: *Prinzipien für die Erfassung realer Leitlinien bei der landwirtschaftlichen Feldarbeit.*

Prinzip	Sensorik	Beispiel
mechanisch	Kontaktschalter, Kraftmesser oder taktiler Taster	Lenkautomatik durch Ertasten der Pflanzenreihen im Mähdrescher- oder Häckslervorsatz bei der Maisernte [61, 62]
optisch	Laufzeitmessung reflektierter Laserstrahlen	Bestandskante von Getreide gegenüber der abgeernteten Fläche [63, 64]
	Kameraerfassung (Vergleich bewachsene/unbewachsene Bereiche)	Bestandskantenerkennung bei der Maisernte [65]
akustisch	Abstandsmessung durch linienförmig angeordnete Ultraschallsensorik	Schwaderkennung von Halmgut und Bestimmung des Flächenschwerpunkts [66]
	Abstandsmessung durch punktförmig angeordnete Ultraschallsensorik	Bestimmung des Abstands des Pflugrahmens zur Furchenkante beim Onlandpflügen [67, 68]

Bei der Navigation nach **virtuellen Leitlinien** wird der Sollkurs nicht direkt aus sensorisch gewonnenen Umgebungsdaten eingeregelt, sondern vorher durch Strategie festgelegt. Die meist verbreiteten Systeme sind satellitengeführt und erhalten ihre augenblickliche Position durch das Differential Global Positioning System (DGPS). Im Unterschied

zum Basissystem GPS werden beim DGPS auf unterschiedliche Arten bezogene Referenzsignale[1)] zusätzlich herangezogen, um die Abweichungen des amerikanischen GPS zur tatsächlichen Ist-Position herauszurechnen. Genauigkeiten im Zentimeterbereich werden so realisiert. Zusätzliche Sensoren, wie z. B. (faseroptische) Kreisel, translatorische und rotatorische Beschleunigungsaufnehmer, Positionsbestimmung aus Lenkwinkel und Ist-Geschwindigkeit ermöglichen Plausibilisierung der Positionsbestimmung bei zeitweiligem Signalverlust, z. B. durch Abschattung oder ähnliches, und kompensieren systematische Fehler, wie die Neigung der Arbeitsmaschine am Hang. Der Abgleich inertialer Positioniersysteme mit der DGPS-Technik wurde von Klee wissenschaftlich untersucht und in einem Sicherheitssystem für Landmaschinen verwendet [69].

Die Hauptintentionen aktueller automatischer Spurführungssysteme (Beispiele in [70-75], Übersichten in [41, 76]) bei der landwirtschaftlichen Reihenfahrt sind

- die Entlastung des Fahrers,
- die Erhöhung der Genauigkeit der Navigation,
- die Erhöhung der Maschinenauslastung,
- die verfahrenstechnische Verbesserung der Applikation.

Das zukünftig verfügbare zivile europäische GPS „Galileo“ [77] wird die Verbreitung satellitengeführter Systeme durch zusätzliche Vorteile, wie geringere Kosten, höhere Verfügbarkeit und bessere Genauigkeit des Basissystems weiter verbreiten.

Weiterführende Konzepte schließen das Wenden am Feldende und die Gerätesteuerung durch automatische Betätigung der Hubwerke und hydraulischen Zusatzventile mit ein [78, 79]. Durch eine solche Verbindung automatisch geregelter Fahrfunktionen mit dem elektronischen Eingriff in den Arbeitsprozess wurde das Potenzial für komplett autonom arbeitende Arbeitsmaschinen geschaffen.

2.2.2 Automatisierung von Arbeitsprozessen

Die Arbeitsprozesse bei mobilen Arbeitsmaschinen erstrecken sich auch außerhalb der Landtechnik auf ein weites Spektrum unterschiedlicher Anwendungsgebiete, z. B. Erd- und Felsbewegung von Tunnelbaumaschinen bis hin zu Kommunalmaschinen beim Reinigungseinsatz von Leitpfosten auf der Autobahn. Wichtigster Vertreter verwendeter Technologien ist dabei die Ölhydraulik. Positive Eigenschaften, wie freizügige Anordnung aller Bauteile, hohe Leistungsdichte, einfache Bewegungsumkehr, stufenlose, nahezu formschlüssige Übersetzungsänderung – um nur einen Teil aus [80] zu nennen – sind maßgeblich für die Verwendung hydraulischer Antriebe bei mobilen Arbeitsmaschinen verant-

1) Üblich sind fest vermessene Referenzstationen, die ihre Korrektursignale über Funk, Mobilfunk oder UKW an das Navigationssystem übertragen.

wortlich. Zusätzlich sind die hydraulischen Aktoren, wie Pumpen, Motoren und Ventile, leicht elektronisch anzusteuern bzw. zu regeln, so dass die meisten Prozessautomatisierungen im mobilen Bereich mit elektrohydraulischer Antriebstechnik bewerkstelligt werden.

Elektrohydraulische Prozessregelung einzelner Systeme

Die Programmierung elektronisch ansteuerbarer Ventile unter Verwendung zusätzlicher Sensorik ermöglicht (Teil-)Automatisierungen von hydraulisch angetriebenen Arbeitsprozessen. Beispiele für Anwendungen bei Traktoren sind sich oft wiederholende Abläufe beim Frontladen, wie Schaufelrückführung in die Ausgangsposition, positionsgeregelte hydraulische Parallelführung des Werkzeugs, Ausschüttelautomatik oder automatisches Ankippen der Schaufel nach der Schüttgutaufnahme [41]. Im Baumaschinenbereich gibt es speziell für Radlader ähnliche Entwicklungen mit zum Teil weiterführender Funktionalität, wie z. B. elektronische Anschläge für Hub- und Anbauwerkzeug, Drehzahlanhebung des Dieselmotors proportional zu den Steuersignalen der Arbeitshydraulik und frei speicherbare Positionen für Hubwerk und Schaufel für wiederkehrende Arbeitsbewegungen [81]. Prozessautomatisierungen bei Kommunalfahrzeugen finden sich z. B. für Positionssteuerungen von Mähwerken, wo der Mähkopf mit konstantem Bodendruck als Regelgröße über die Auflagefläche geführt wird und so der Bodenkontur automatisch folgt [82].

Die Dreipunktverbindung zwischen Traktor und angebautem Gerät wurde in den letzten Jahren regelungstechnisch ständig weiterentwickelt. Erste Systeme der elektronisch-hydraulischen Hubwerksregelung (EHR) regelten nur die Zugkraft und/oder die Soll-Position des Gerätes durch Heben und Senken des Heckkrafthebers. Später wurden Systeme für aktive Schwingungsdämpfung zur Ausregelung der Radlastschwankungen an der Vorderachse, durch Verarbeitung von Position und Unterlenkerkraft, Stand der Technik [83]. Der elektronisch geregelte, hydraulisch verstellbare Oberlenker erweitert erneut die Funktionalität des Heckdreipunktanbaus durch Möglichkeiten zum Parallel- oder Steilaushub der angebauten Geräte. Durch zusätzliche Einführung von elektrohydraulisch längengeregelten Hubstreben werden die Steuerungsmöglichkeiten von Anbaugeräten weiter verbessert, siehe auch [84]. Ein völlig neues Konzept ist die Realisierung des Heckanbaus durch eine vertikal gestellte Stewart-Plattform[1)] mit sechs gleichen hydraulischen Zylindern in Hexapodanordnung zwischen Traktor und Gerät, wie es in [86] vorgestellt wird. Durch geschickte Regelung der Zylinderlängen, die durch integrierte Sensoren erfasst werden, erreicht man sechs Freiheitsgrade für die Bewegungen der Geräteschnittstelle und damit ein äußerst hohes Automatisierungspotenzial.

Ein geräteseitiger Ansatz liegt im Konfigurationsmanagement landwirtschaftlicher Geräte durch elektronische Einstellmöglichkeiten und Datenverwaltung für hydraulische

1) Parallelkinematik mit sechs Freiheitsgraden nach Stewart [85].

Funktionen. Einmal am Traktor zentral gespeicherte Konfigurationsdaten der Zusatzhydraulik erlauben Zugriff und automatisches Einstellen der gerätespezifischen Prozessparameter zum späteren Zeitpunkt. Beispielsweise sind die hydraulischen Verstellfunktionen von Anbaupflügen für den Fahrer bequem aus der Kabine per Terminal konfigurier- und verwaltbar oder werden vom Gerät selbst automatisch abgerufen und dem Fahrer vorgeschlagen [87, 88].

Für die Automatisierung mehrerer hydraulischer Funktionen durch einen Geräterechner geht man einen Schritt weiter. In einem Konzept der Firma Reichhardt Steuerungstechnik können sämtliche Betätigungen eines 9-scharigen Aufsattelpflugs (Fa. Vogel & Noot) auf jeweils einen Tastendruck für das Ausheben und Einsetzen reduziert werden. Das Ausheben, Wenden und erneute Einsetzen großer Aufsattelpflüge erfordert zahlreiche koordinierte Betätigungen der Traktorhydraulik und eine hohe Beanspruchung für den Fahrer. Zusätzlich zum Wenden unterstützt die Automatik bei der Reihenfahrt. Ein Ultraschallsensor erfasst die letzte Furche und ermöglicht so die Regelung der Querauslenkung zum Traktor, siehe [68].

Arbeiten mobile Maschinen häufig in hügeligem oder sogar steilem Gelände und wird durch die Schrägstellung die Fahrstabilität oder die Erledigung des Arbeitsprozesses negativ beeinflusst, werden teilweise aktive Ausgleichsysteme eingesetzt, welche die seitliche Hangneigung bzw. die Steigung oder das Gefälle in Längsrichtung automatisch ausgleichen. Die Neigung der Maschine wird durch eine fahrwerksfeste, elektronische Wasserwaage erfasst und über aktives Kippen relevanter Maschinenteile, des Maschinenoberwagens oder der gesamten Maschine ohne Fahrwerk zum Hang hin ausgeregelt.

In der Landtechnik wird dieses Prinzip bei Mähdreschern zur Sicherstellung der Arbeitsqualität bei der Körner/Stroh-Trennung angewandt. Verschiedene Hersteller bieten Hangausgleichsysteme an, bei denen die gesamte Maschine durch Verschränkung der Endantriebe des Fahrwerks nach oben oder unten eine Schrägstellung relativ zum Fahrwerk erfährt. Abhängig von der Hangneigung wird der Mähdrescher und damit die Dreschtechnik und Reinigungsanlage geneigt und gleiche Effektivität wie in der Ebene sichergestellt. Seitenneigungen bis zu 20% und Gefälle bis zu 6% werden so ausgeglichen. Das gesamte Schneidwerk folgt sekundär abstandsgeregelt der Bodenkontur [89, 90]. Ein Beispiel aus der Kommunaltechnik ist der selbstfahrende Böschungsmäher der Firma Etesia [91]. Durch hintereinander angeordnete Triebräder und zum Hang verschiebbare seitliche Stützräder beherrscht er Hanglagen bis zu 34°. Besonders in der Forsttechnik werden höchste sicherheitstechnische Anforderungen an automatische Hangausgleichsysteme gestellt. Wo extreme Steigungen, stark schwankendes Geländeprofil und starker Bewuchs die Arbeitsbedingungen erschweren, verbessert der automatische Hangausgleich

die Fahrstabilität, wie es in [92] für die Anwendung eines Kompaktharvesters beschrieben wird.

Ablaufsteuerungen und -regelungen übergeordneter Systeme bei Landmaschinen

Landmaschinen bieten einige Beispiele für übergeordnete Prozessautomatiken in Form von Ablaufsteuerungen und -regelungen, bei denen die Automatisierung mehrerer Teilsysteme zu einer übergeordneten, ineinander greifenden Funktionalität kombiniert wird. Ein Hauptanwendungsbereich ist der Wendevorgang einer Traktor/Geräte-Kombination am Feldende, dem so genannten Vorgewende[1)], wo für den Fahrer sehr viele Betätigungen und Handgriffe anfallen. Zur Unterstützung des Fahrers werden Eingriffe in den Antriebsstrang, Betätigung der Hubwerke vorne und hinten, Schalten der Zapfwelle und Steuerung der Zusatzhydraulik – also traktorinterne Betätigungen sowie externe Schnittstellenbeschaltung – automatisch vollzogen. Bei einer Saatbettkombination aus Drillmaschine, Frontpacker, Kreiselegge zusammen mit einem Standardtraktor ergeben sich beispielsweise 16 Arbeitsschritte für das Ausheben, Wenden und erneute Einsetzen der Geräte, welche die Fahrfunktionen des Traktors und die Schnittstellen zwischen Traktor und Geräten betreffen: Fronthubwerk ausheben, Drillmaschine ausheben, Heckhubwerk ausheben, Zapfwelle ausschalten, Differentialsperre ausschalten, Gas wegnehmen, Herunterschalten, ..., bis zum erneuten Einsetzen des Spuranreißers und Einschalten der Differentialsperre [93]. Die hohe Anzahl von Arbeitsschritten am Vorgewende, gerade bei komplexen Traktor/Geräte-Kombinationen, bieten damit höchstes Automatisierungspotenzial für Wendevorgang, Einsetzen und Ausheben der Geräte [94].

Im Rahmen des Forschungsprojektes „Traktormanagementsysteme“ [32, 33] wurde zusätzlich zur Regelung des Antriebsstrangs ein anwendungsbezogenes Feldendemanagement realisiert, das den Fahrer durch zeitgesteuerte Automatisierung der Aufgaben Absenken der Motordrehzahl, Pflugausheben, Pflugdrehen und Pflugeinsetzen erheblich entlastet [95]. Am Markt erhältlich sind weiterentwickelte so genannte Vorgewende-Management-Systeme, wo der Fahrer beliebige Arbeitsschritte eines Arbeitsprozesses bezüglich hydraulischer Zusatzventile, Zapfwellen, Hubwerke, Wahl der Fahrgeschwindigkeit und der Motordrehzahl frei auswählen und in einer Datenbank im Traktor ablegen kann. Bei Bedarf können die abgespeicherten Abfolgen im Konzept der Firma AGCO-Fendt [96, 97] weg-, zeit- oder ereignisgesteuert, abhängig von Hubwerksstellung oder Knopfdruck, im Konzept der Firma Deutz-Fahr [98, 99] rein ereignisgesteuert durch Tasterbetätigung abgerufen werden. Weitere Systeme bieten New Holland (zeitgesteuert), John Deere und Case IH (beide weggesteuert) an. Eine Übersicht der gängigen Systeme bietet [93].

---

1) Am Rand des Feldes befindlicher Streifen, an dem die landwirtschaftlichen Maschinen gewendet werden.

Noch einen Schritt weiter gehen die schon unter Kapitel 2.2.1 erwähnten autonom fahrenden und prozessautomatisierten Arbeitsmaschinen, die durch intelligente Elektronik (Teil-)Prozesse bei der Arbeitserledigung vollständig automatisieren, siehe dazu noch mal [78, 79]. Dem Fahrer überbleibt dann lediglich die Aufgabe, die Applikation der Arbeitserledigung, z. B. die landwirtschaftlichen Geräte bei Bodenbearbeitung oder Bestellung, zu kontrollieren und das Gesamtsystem sicherheitstechnisch zu überwachen.

Nach Auernhammer leiten sich aus den heute schon realisierten und zukünftig realisierbaren Systemen der Feldrobotik folgende Entwicklungslinien ab, die einen zunehmenden Wegfall manueller Bedien- und Überwachungsfunktionen ermöglichen [2, 100]:

- **Bemanntes Führungsfahrzeug mit unbemannten Drohnen**, z. B. für die Kombination von Saatbettbereitung und Sätechnik oder Erntemaschinen mit unbemannten Folgemaschinen.
- **Unbemannte, autonome Fahrzeuge herkömmlicher Bauart**, z. B. für monotone Tätigkeiten auf großen Flächen (Pflügen) oder hohes Automatisierungspotenzial.
- **Feldroboter in spezialisierter Bauart**, welche niedrigste Bodenbelastungen, umweltschonende Energiesysteme oder optimierte Werkzeuge und Geräte ermöglichen. [101] zeigt ein interessantes Beispiel.

Hinsichtlich der Kombination von Fahrzeugführung und Erledigung des Arbeitsprozesses weisen Landmaschinen mit das höchste Automatisierungspotenzial innerhalb der mobilen Arbeitsmaschinen auf. Auch deswegen können die besonderen Eigenschaften dieser Systeme sicherheitstechnisch als beispielhaft für andere mobile Arbeitsmaschinen gesehen werden.

2.2.3 Komponenten, Subsysteme, vernetzte Systeme

Bei der Entwicklung sicherheitsrelevanter mechatronischer Systeme von mobilen Arbeitsmaschinen können die Erfahrungen aus dem Automotive-Bereich hilfreich sein. Die Auswahl der Komponenten und Subsysteme sowie ihre vernetzte Anordnung sind dabei wichtige Faktoren für eine sicherheitsgerechte Auslegung bis hin zu fehlertoleranten Systemen (siehe auch Kapitel 3.2). Zukünftige Entwicklungen bei Kfz, wie z. B. die Erweiterung bestehender Längsführungssysteme durch automatische Notfallbremsung [102], Erfassung des Fahrzeugumfelds durch Radartechnik und optische Systeme [103, 104] und damit mögliche Unterstützung des Fahrers durch automatische Querführung [105] machen die Notwendigkeit funktionssicherer Systeme deutlich, zeigen aber auch Anwendungsmöglichkeiten für mobile Arbeitsmaschinen. Im Folgenden werden etablierte Systemkomponenten und mögliche Architekturen, auch mit Anregungen aus dem Bereich der Pkw und Nkw im Hinblick auf die Systemsicherheit und -zuverlässigkeit gezeigt.

Komponenten und Subsysteme

Die Zuverlässigkeit eines Systems wird in großen Teilen durch die Zuverlässigkeiten seiner Komponenten bzw. Teilsysteme sowie durch seine Architektur bzw. Struktur bestimmt. Möchte man von den elektronischen Systemen bei Kfz profitieren, liegt das größte Potenzial im Bereich der **Sensoren und Aktoren**, die grundsätzlich unerlässlich für den Aufbau mechatronischer Systeme sind, siehe zuvor Bild 2-2. In sicherheitskritischen Systemen verwendet man mehr und mehr fehlertolerante Sensoren, die durch mehrkanalige Messwerterfassung das rechtzeitige Diagnostizieren eines Fehlers ermöglichen und das System weiterhin verfügbar halten (Ein-Fehler-Sicherheit). Dies wird durch unabhängige redundante Strukturen erreicht, wie z. B. Erfassung von Kraft und Weg bei Betätigung eines Fahrpedals oder berührungslos arbeitende, induktive Positionsaufnehmer mit zwei galvanisch getrennten Signalwegstrukturen [106]. Die integrierte Bauweise berührungsloser Konzepte beugt Fehlmontage oder Kalibrierungsfehlern vor und ist unempfindlich gegen Verschmutzung und Verschleiß [107]. Einen Überblick gebräuchlicher Sensoren im Kfz und zukünftige Sensortechnologien, gerade für sicherheitsrelevante Anwendungsfälle, finden sich in [108] und [109].

Bei Betätigungseinheiten für X-by-Wire-Systeme ergeben sich Zusatzaufgaben auf Grund der fehlenden mechanischen Rückmeldung der Systemantwort an den Fahrer. Das subjektiv empfindbare Betätigungsverhalten der Mensch-Maschine-Schnittstelle, z. B. Fahrhebel, Steer-by-Wire-Lenkrad oder Joystick für hydraulische Funktionen, muss durch eine eigene integrierte Aktorik simuliert werden. Der Sollwertgeber wird damit zur intelligenten Sensor/Aktor-Einheit erweitert. Das elektrohydraulische Bremssystem für die Mercedes-Benz E-Klasse simuliert beispielsweise das Pedalverhalten für den Fahrer durch einen angepassten Verlauf der Pedalkraft über dem Pedalweg, um ein optimales Bremsgefühl zu erhalten [110]. Sollwertgeber mit aktiven, simulierten Rückmeldungen an den Fahrer sind auch bei Baumaschinen verbreitet, wie z. B. elektrohydraulische Stellhebel mit Force-Feedback.

Bei der Auswahl von **elektronischen Steuergeräten** für mobile Arbeitsmaschinen geht man bedingt durch Stückzahlenunterschiede und verschiedene unternehmerische Strukturen grundsätzlich zweierlei Wege: Bei geringen Stückzahlen werden oft universell programmierbare ECUs mit Standardlösungen für Prozessor, Speicher und Ein-/Ausgänge eingesetzt – im Gegensatz zu den speziell konfektionierten, an den konkreten Anwendungsfall angepassten Rechnern, die erst bei mittlerer und hoher Stückzahl Rentabilität versprechen. Die Vorteile proprietär konfektionierter Hardware liegen in höherer Gestaltungsfreiheit beim Layout und zukunftssicherer Verfügbarkeit, wenn auch die hohen Stückzahlen des Automobil-Bereichs nicht erreicht werden. Es gibt allerdings Ansätze in der Automobilindustrie, zukünftig universell ausgelegte, standardisierte Steuergeräte mit

zukunftssicherer Verfügbarkeit und Performance zu entwickeln und herstellerübergreifend zugänglich zu machen. Für Hersteller mobiler Arbeitsmaschinen ergäbe sich somit die Chance, auf standardisierte Hardware zurückzugreifen, die in deutlich höheren Stückzahlen aufgelegt und den Anforderungen an Steuergeräte für den mobilen Einsatz gerecht wird. Aufgrund steigender funktionell und sicherheitstechnisch begründeter Anforderungen an die Prozessorleistung werden wohl mittelfristig Systeme mit 32 Bit-Technologie (u. U. mit Fließkomma-Arithmetik) die häufig auf 16 Bit-Mikrocontroller basierenden Standardsysteme mit Ganzzahl-Arithmetik ablösen. Wo erforderlich, kann man sicherheitstechnisch die nötige Fehlertoleranz durch mehrkanalige Anordnung oder Rückfallebenen, auch hinsichtlich der Spannungsversorgung, erreichen. Lösungen siehe in [111].

Architektur vernetzter Systeme

Ein Großteil des Datenaustauschs komplexer Funktionalitäten bei mobilen Maschinensystemen wird mittlerweile durch elektronische Kommunikationssysteme gelöst und ist damit deutlich einfacher darstellbar, siehe auch [112]. Stand der Technik bei seriellen Kommunikationssystemen sind CAN-Netzwerke [113], anfangs zwischen Motor und Getriebe [114], später auch unter Einbeziehung von Komfortfunktionen, Zusatzhydraulik oder Fahrerschnittstelle, [115]. Mittlerweile bauen höherschichtige Kommunikationsprotokolle auf den unteren Schichten des CAN-Standards auf und standardisieren die anwendungsspezifische interne wie externe Datenkommunikation. Die fahrzeuginterne Kommunikation zwischen Motor, Getriebe und Zusatzaggregaten wird oftmals über das Protokoll SAE J1939 [116] geregelt, das aus dem amerikanischen Nutzfahrzeugssektor stammt. Ein zusätzlich systemübergreifenderer Ansatz stammt aus der Landtechnik und wird im internationalen Normungsprojekt ISO 11783 [117], auch genannt ISOBUS, bearbeitet. Das genormte Kommunikationsprotokoll soll elektronische Steuerrechner oder Terminals unterschiedlicher Maschinen, Geräte und Hersteller zusammenführen [118] und findet auch bei Kommunalmaschinen Einsatz [119]. Im Baumaschinenbereich wurden, basiert auf dem offenen Kommunikationsprotokoll für Industriemaschinen CANopen [120], Geräteprofile standardisiert, welche die Kombination von elektronischen Steuergeräten, Sensorik, Aktorik und Mensch-Maschine-Schnittstelle in den Gesamtsystemen erheblich erleichtern sollen [121]. Bezüglich der definierten Übertragung von Diagnosedaten über CAN-Systeme sind zwei relevante Standards ISO 14230 und SAE J 1939/73 [122, 123] in Anwendung, die in einem aktuellen ISO-Normungsprojekt ISO/DIS 15765 zusammengeführt werden sollen [124]. In [125] wird ein diesbezügliches Beispiel für die Diagnose im breiten Feldeinsatz der Serie vorgestellt.

Für sicherheitsrelevante Systeme ist es unter Umständen notwendig, die Datenkommunikation fehlertolerant zu gestalten. Grundsätzlich gibt es dafür zwei Ansätze: Einmal durch Erweiterung bestehender nicht-fehlertoleranter Systeme zu mehrkanaligen Struktu-

ren, zum anderen das Zurückgreifen auf neu entwickelte BUS-Derivate, die sich Fehlertoleranz als Ziel gesetzt haben. Ein weiterer sicherheitstechnischer Aspekt ist die Unterscheidung nach ereignis- und zeitgesteuerten Systemen und damit indirekt nach der Verfügbarkeit des Kommunikationssystems. Vorteil der zeitgesteuerten Architektur ist die deterministische Abarbeitung der Kommunikationsprozesse, d. h. es ist jederzeit eindeutig, welche Daten „wo und wie“ kommuniziert werden. Überlastungen und Engpässe des Kommunikationssystems durch schnell aufeinander folgende Ereignisse, wie sie bei ereignisgesteuerten Systemen z. B. CAN möglich sind, werden dadurch vermieden. In **Tabelle 2-5** werden gebräuchliche Kommunikationssysteme für verteilte Systeme gezeigt und nach den wichtigsten (sicherheitstechnischen) Kriterien unterschieden.

Tabelle 2-5: *Übersicht über Kommunikationssysteme für die Vernetzung elektronischer Steuergeräte (Standards teilweise noch in Entwicklung).*

Kriterium	**CAN low-speed**	**CAN high-speed**	**TTCAN**	**TTP**	**FlexRay**
Kommunikationsablauf	ereignisgesteuert	ereignisgesteuert	zeitgesteuert (anteilig ereignisgesteuert)	zeitgesteuert	zeitgesteuert mit dynamischem Ereigniskanal
max. Übertragungsrate	0,125 Mbit/s	1 Mbit/s	1 Mbit/s	5-25 Mbit/s	10 Mbit/s
BUS-Last	max. 58 %, typisch ca. 30 %	max. 58 %, typisch ca. 30 %	max. >58 %, typisch >30 %	max. 90 %, typisch >60 %	max. 95 %, empf. 40-60 %
Fehlertoleranz	ja (1-Drahtbetrieb physikalisch möglich)	nein	nein	ja (2-kanalige Architektur optional)	ja (2-kanalige Architektur optional)
Vermeidung „Babbling Idiot“ [a)]	nein	nein	nein	ja	ja
Fehlerdiagnose	gut, Wiederholung fehlerhaft gesendeter Nachrichten		sehr gut, erkennt Bit-, Sende- und Empfangsfehler		sehr gut, erkennt Bitfehler
Typisches Anwendungsbeispiel	Komfortelektronik z. B. Klimaanlage	Antriebsstrang z. B. Motor, Getriebe	auf CAN basierte kritische Systeme	hochkritische Systeme, z. B. Steer-by-Wire	kritische Systeme, z. B. Brake-by-Wire
Referenz	ISO 11898-1 u. 3 [126]	ISO 11898-1 u. 2 [126]	ISO 11898-4 [126], [127]	[128, 129]	[130, 131]

a) Blockierung der Kommunikation durch ständig fehlerhaft sendenden BUS-Teilnehmer (BUS-Monopolisierung).

Aus oben genannten Gründen ist der zeitgesteuerten Architektur für sicherheitsrelevante Anwendungen Vorzug zu geben. Die Möglichkeit vollwertiger Fehlertoleranz durch 2-kanaligen Betrieb ist nur bei TTP und FlexRay, einer Weiterentwicklung des im BMW 5er realisierten Kommunikationssystems Byteflight [132], im Protokoll vorgesehen. Das auf

CAN basierende TTCAN vereint die zeitgesteuerte Architektur mit ereignisgesteuerten Kommunikationsrahmen, wodurch eine Abwärtskompatibilität zu normalen CAN-Systemen gewährleistet wird. Höherschichtige Protokolle (z. B. CANopen oder ISO 11783) können somit mit dem Vorteil der deterministischen Kommunikation oder auch weiterhin ereignisgesteuert gefahren werden. Für die Fehlereindämmung im Zeitbereich, z. B. BUS-Monopolisierung, sehen TTP und FlexRay so genannte BUS-Guardians vor – unabhängige Instanzen, welche die Teilnehmer überwachen und bei Bedarf vom Kommunikationsmedium trennen – und können so in Verbindung mit einer 2-kanaligen Struktur vollwertige Fehlertoleranz erreichen. In [133] werden zu berücksichtigende Einflüsse für die Entwicklung zeitgesteuerter Systeme dargelegt. Nachteil ist noch die mangelnde Erfahrung im breiten Anwendungsfall. Es bleibt deshalb abzuwarten, wie sich die zeitgesteuerten Protokolle, speziell TTP und Flexray, im Feld etablieren. Low-speed-CAN Systeme sind zwar logisch und physikalisch 2-kanalig ausgelegt, haben aber deutliche Nachteile hinsichtlich Echtzeitfähigkeit bei schnellen Regelvorgängen wegen der geringen Übertragungsrate von max. 125 kbit/s. Will man also die Vorteile zeitgesteuerter Systeme nutzen aber nicht auf etablierte Kommunikationsstandards verzichten, könnte der TTCAN-Standard in Verbindung mit einer ausfallsicheren, fehlertoleranten Netzwerkstruktur als Empfehlung für sicherheitskritische Systeme bei mobilen Arbeitsmaschinen gelten.

Durch geschickte Netzwerkarchitektur können auch im eigentlichen Sinne 1-kanalig arbeitende Systeme zu fehlertoleranten erweitert werden, siehe [134]. Ein Ansatz für redundante CAN-Kommunikation mit hoher Übertragungsrate (1MBit/s) wird in [135] vorgestellt. Eine andere Lösung aus dem Kfz-Bereich verwendet dynamische Funktionsverlagerung zur Fehlerbehandlung in vernetzten Systemen. Kommt es zum Ausfall einer Funktion oder Komponente, kann bedarfsorientiert eine andere Einheit die entsprechende Lücke füllen, [136].

2.3 Entwicklungsprozesse und -modelle

Die Entwicklungsprozesse für mechatronische Systeme bei mobilen Arbeitsmaschinen orientieren sich, bedingt durch die steigende Komplexität, zunehmend an der Pkw- und Nutzfahrzeugindustrie. Für die mittelständisch geprägten Unternehmensstrukturen des behandelten Industriezweigs ist ein stückzahlengerechter Entwicklungsaufwand damit aber schwer zu erreichen. Die im Folgenden vorgestellten Entwicklungsprozesse und systemübergreifenden Entwicklungsmodelle sollen den Stand der Technik im Automotive-Bereich beleuchten und als Grundlage für einen später in der Arbeit beschriebenen Leitfaden für die Entwicklung elektrisch/elektronisch/programmierbar elektronischer Systeme (E/E/PES) von mobilen Arbeitsmaschinen dienen. Speziell an die Anwendungsfälle bei

mobilen Arbeitsmaschinen angepasste Entwicklungskonzepte, insbesondere mit Hinblick auf die funktionale Sicherheit der Systeme, sind dem Autor nicht bekannt.

2.3.1 Konventionelle Vorgehensweise

In den konventionellen Entwicklungsprozessen werden die einzelnen Teilsysteme oft getrennt voneinander entwickelt und später, unter genauen Schnittstellenvorgaben, in das Gesamtsystem integriert. Eine **asynchrone** Entwicklung von Teilsystemen ist damit möglich. Innerhalb der Teilsysteme nimmt die Software einen immer größeren Anteil der Funktionalität der Systeme ein. Eine Trennung der Entwicklungsprozesse für Software und hardwarelastige Systemelemente muss aber vermieden werden. Design und Konzeption von Software- und Hardwaremodulen sind parallel anzugehen. In **Bild 2-3** wird ein Beispiel für einen konventionellen Entwicklungsprozess für E/E/PE-Systeme gezeigt.

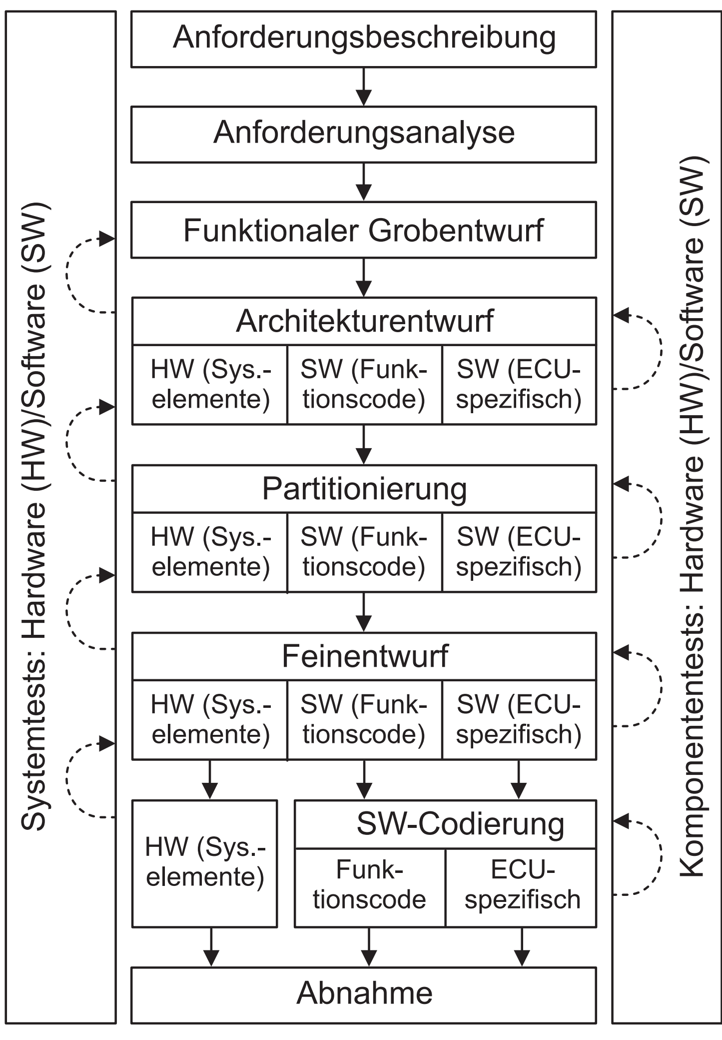


Bild 2-3: *Konventioneller Entwicklungsprozess für elektrisch/elektronisch/programmierbar elektronische Systeme (E/E/PES).*

Die Entwicklung eines mechatronischen (Teil-) Systems beginnt mit der Beschreibung der Anforderungen hinsichtlich Funktionalität und Rahmenbedingungen im Gesamtsystem. In der Anforderungsanalyse wird die Anforderungsliste auf systematische Zusammenhänge und Einzelfunktionen umgebrochen. Daraufhin bestimmt der funktionale Grobentwurf die Systemstruktur durch Aufteilung der Funktionen und Festlegung der internen Schnittstellen. Der Architekturentwurf unterteilt das Pflichtenheft in Hardware- und Softwareanforderungen und fixiert dabei die Eigenschaften der Systemelemente für Informationsverarbeitung und intelligente Sensorik bzw. Aktorik. Die Verteilung der Funktionen auf die einzelnen Subsysteme geschieht in der Partitionierung auf konkrete Steuereinheiten. Aufgabe des Feinentwurfs ist es, den Funktionscode

der einzelnen Steuereinheiten, die Sicherstellung der Funktionalität auf Betriebssystemebene und das Konzept der Datenkommunikation festzulegen. Die eigentliche Codierung der Software und Integration auf die Zielhardware erfolgt zuletzt und schließt die Entwicklung ab. Der gesamte Ablauf wird von Tests auf Komponenten-, System- bzw. Subsystemebene begleitet, welche Iterationen innerhalb der einzelnen Entwicklungsschritte und unter Umständen zurück in die vorherige Entwicklungsphase erforderlich machen können. Grundsätzlich gilt es, phasenübergreifende Iterationen möglichst zu vermeiden.

Der Entwicklungsprozess hat zusätzlich die Aufgabe, den organisatorischen Rahmen anhand folgender Kriterien festzulegen:

- die durchzuführenden Entwicklungsaktivitäten und deren Reihenfolge
- die jeweils entstehenden Teilprodukte
- die anzuwendenden Standards, Methoden und Werkzeuge
- den notwendigen Dokumentationsumfang
- die Verteilung der Verantwortlichkeiten
- die Abnahme- und Fertigstellungskriterien

Aktuelle Ansätze verlassen die klassische Linienstruktur und ordnen Spezifikations- und Testphasen der einzelnen Entwicklungsstände gegenseitig zu. Etabliert hat sich das so genannte V-Modell (Vorgehensmodell). Ursprünglich handelt es sich um einen Entwicklungsstandard für IT-Systeme des Bundes [137]. Mittlerweile wird das V-Modell in vielen Bereichen zur Entwicklung von E/E/PE-Systemen verwendet und beschreibt den Weg von der Systemspezifikation bis zur Validierung über unterschiedliche Detaillierungsebenen, siehe **Bild 2-4**.

Die aus der Anforderungsanalyse erarbeiteten Funktionen werden auf unterschiedliche Funktionseinheiten logisch partitioniert und später auf die nötigen Subsysteme verteilt. Die eigentliche Umsetzung der Funktionsstrukturen in Form von Serien-Code geschieht im unteren Teil des V-Modells, der Softwareentwicklung. Den einzelnen Entwicklungsschritten sind unterschiedliche an den entsprechenden Anwen-

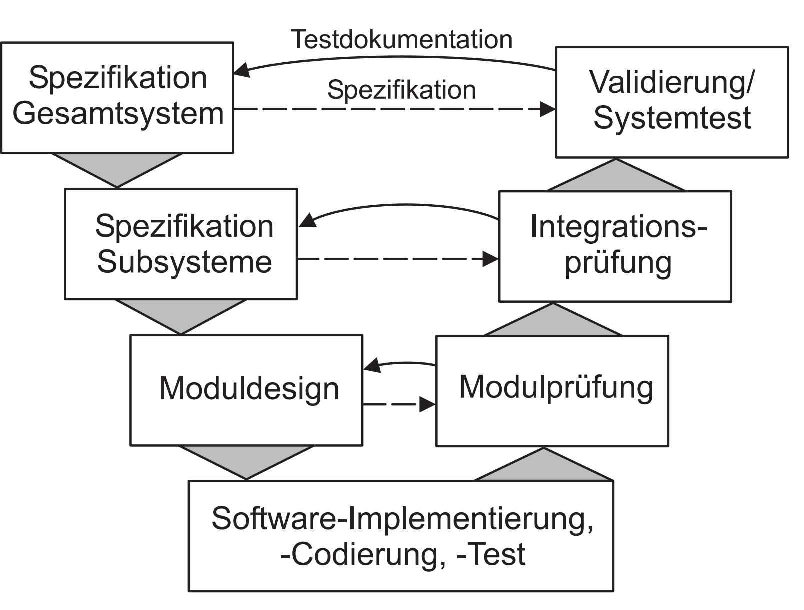


Bild 2-4: *Das V-Modell für Entwicklungsprozesse von mechatronischen Systemen.*

dungsfall angepasste Entwicklungs- und Testmethoden zugeordnet. Die Testdurchläufe der rechten Seite des V-Modells überprüfen die entsprechenden Spezifikationsanforderungen auf der linken Seite.

2.3.2 Verteilte Entwicklung verteilter Systeme

Die steigende Komplexität der Systeme, insbesondere die immer größer werdende Anzahl der elektronischen Steuergeräte und verteilten Funktionalitäten, hat eine zunehmend notwendige Spezialisierung der OEM (Original Equipment Manufacturer) zur Folge. Immer mehr wird die Entwicklungsverantwortung einzelner Teilsysteme dem Zulieferer übertragen (Outsourcing). Einzelne Teile der Entwicklungsprozesse sind deshalb aber für den OEM teilweise nicht mehr einsehbar oder nachvollziehbar. Um Schnittstellenprobleme zu vermeiden, ist eine asynchrone Entwicklung von Teilsystemen **nicht** mehr möglich. Die Synchronisation der verteilten Entwicklung des Systemverbunds erfordert jedoch die Kenntnisse der Entwicklungsprozesse bei den verschiedenen Lieferanten und die Möglichkeit für den OEM, auf Ereignisse der einzelnen Entwicklungsphasen zurückgreifen zu können, siehe auch [138].

Wichtiger Aspekt transparenter Entwicklungsvorgänge beim Lieferanten ist die Quantifizierbarkeit der Entwicklungsprozesse. Da die Softwareentwicklung diesbezüglich die größte Herausforderung darstellt, sozusagen am schlechtesten messbar ist, setzen die Hersteller Assessmentverfahren zur Bestimmung des Reifegrads und Identifikation des Verbesserungspotentials von Softwareprozessen ein, z. B. Software-Audit nach ISO/IEC 15504 [139], auch bekannt als SPICE (Software Process Improvement and Capability Determination). Vorgefertigte, mehrstufige Beurteilungsschemata dienen sowohl zu einer unternehmensübergreifend vergleichbaren Bestandsaufnahme des Ist-Zustands als auch zur Etablierung eines Verbesserungsprogramms. Das weiterentwickelte Prozessmodell CMMI [140] (Capability Maturity Model Integration) hat den gleichen Ansatz, ist aber nicht rein an Softwareentwicklung gebunden und lässt mehr anwendungsspezifische Freiheiten. **Tabelle 2-6** zeigt die fünf aufeinander aufbauenden Reifegradstufen für Prozesse. Die Bewertung wird mit Hilfe von Fragebögen bzw. Kriterienkatalogen, so genannten Assessments, durchgeführt.

Mit Hilfe der ermittelten Reifegradstufe kann die Softwareprozessfähigkeit eines Lieferanten oder auch der eigenen Entwicklungsabteilung standardisiert nachgewiesen werden, um die Schwierigkeiten der verteilten Entwicklung zu entschärfen und qualitativ ausgereifte und sicherheitsgerechte Systeme zu gewährleisten.

Tabelle 2-6: *Durch Assessment festgestellte Reifegrade von Entwicklungsprozessen gemäß CMMI [140]. Für eine definierte Reifegradstufe müssen alle Forderungen einschließlich die der niedrigeren Stufen erfüllt sein.*

CMMI		**Beschreibung**
Reifegrad	5	Optimierend (Kontinuierliche Verbesserung; etablierter Regelkreis für die Messung und Verbesserung der Prozesse; integraler Bestandteil aller Organisationsprozesse)
	4	Quantitativ gemanaged (Nutzung von Metriken und Kennzahlen; instrumentierte Prozessumgebung und -überwachung mit quantitativer Datenerfassung und -verwaltung)
	3	Definiert (Definierte Prozesse für Entwicklung und Management; Teilprozesse zusammengefasst und in unternehmensweites Prozessmodell eingebettet)
	2	Gemanaged (Einfaches Projektmanagement mit entsprechendem Phasenmodell)
	1	Initial (Ad hoc Prozesse ohne formelle Planung und Kontrolle)

2.4 Stand der Normung

Bevor der aktuelle Stand der Normen und Richtlinien für eine sicherheitsgerechte Entwicklung mobiler, mechatronischer Maschinensysteme aufgezeigt werden soll, ist es hilfreich, einen Blick auf die rechtliche Normen- und Richtlinienstruktur in Europa zu werfen. Die Zielsetzung der Europäischen Union (EU) läuft auf den Abbau gegenseitiger Handelshemmnisse hinaus. Bei Kfz und vielen mobilen Arbeitsmaschinen soll dies über harmonisierte Vorschriften und durch ein einheitliches Betriebserlaubnisverfahren erreicht werden. Fahrzeuge mit einer EG-Typgenehmigung werden nur einmal homologisiert, können jedoch freizügig innerhalb aller EU-Staaten verkauft bzw. ohne erneute Prüfung zugelassen werden. Die EG-Typgenehmigung setzt voraus, dass für die einzelnen Systeme, Baugruppen und technischen Einheiten harmonisierte technische Vorschriften geschaffen werden, die als Richtlinie vom Rat der EU beschlossen werden. Die Mitgliedstaaten sind **verpflichtet**, diese EG-Richtlinien in ihr nationales Recht zu übernehmen – sie sind damit für den Hersteller bindend.

Unterhalb der EG-Richtlinien der EU stehen die ECE-Regelungen der UNECE (United Nations Economic Commission for Europe). Sie haben **empfehlenden** Charakter und spiegeln ähnlich wie Normen den Stand der Technik wieder. Die ECE-Regelungen sind nur zwingend anzuwenden, wenn die Straßenverkehrs-Zulassungs-Ordnung (StVZO) [13] oder eine andere Richtlinie ausdrücklich darauf verweist. Oftmals werden ECE-Regelungen, die so für nationales Recht geltend gemacht werden sollen, in EG-Richtlinien umgewandelt – z. B. ist die ECE-Regelung Nr. 13 gleichwertig mit Richtlinie 71/320/EWG „Bremsanlagen".

Die grundsätzlichen Sicherheitsanforderungen der EG-Richtlinien werden in technischen Spezifikationen der internationalen Normung konkretisiert. Alle Normen, wie DIN

auf nationaler, EN auf europäischer und ISO auf internationaler Basis, sollen den Stand der Technik dokumentieren, haben aber **keinen** Gesetzescharakter und sind somit Empfehlungen an den Hersteller. Die Bedeutung der unterschiedlichen Normungsinstitute verschiebt sich immer weiter von nationaler Normung in Richtung EN und ISO. Zur Vereinheitlichung innerhalb der EU ist das Europäische Komitee für Normung (CEN) mit der Erarbeitung harmonisierter europäischer Normen (EN) betraut, die von allen Mitgliedstaaten unverändert als nationale Norm übernommen werden müssen. Entgegenstehende oder davon abweichende nationale Normen sind zurückzuziehen. Der systematische und hierarchische Aufbau wird in drei Normentypen gegliedert:

- **Typ A-Normen**: Sicherheits-Grundnormen über Gestaltungsleitsätze und allgemeine Aspekte, die alle Maschinen in gleicher oder ähnlicher Weise betreffen.
- **Typ B-Normen**: Sicherheits-Gruppennormen über Aspekte, die mehrere oder eine Reihe von ähnlichen Maschinen betreffen oder über sicherheitsbedingte Einrichtungen, die für verschiedene Arten von Maschinen verwendet werden können.
- **Typ C-Normen**: Sicherheits-Produkt- oder -Fachnormen mit konkreten Anforderungen und Schutzmaßnahmen zu allen signifikanten Gefährdungen, die von einer Maschine oder allen Arten einer Maschinengruppe ausgehen.

Hierarchisch stehen die Produkt- oder Fachnormen (Typ C) an der Spitze, d. h. nur wenn für ein System keine Produkt- oder Fachnorm vorliegt, geben die relevanten Gruppennormen (Typ B) oder in letzter Instanz die Grundnormen (Typ A) Entscheidungshilfe.

Bild 2-5 zeigt eine hierarchisch strukturierte Übersicht über die wichtigsten relevanten Richtlinien, Regeln und Normen, welche die Grundlage für einen sicherheitsgerechten Entwicklungsleitfaden für mechatronische Systeme bei mobilen Arbeitsmaschinen bilden. Die zwingend zu erfüllenden EG-Richtlinien 98/37/EG [141] (Maschinenrichtlinie) und 2001/95/EG [142] (Richtlinie zur allgemeinen Produktsicherheit) geben den für den Hersteller bindenden Rahmen vor. Dabei sind diese Richtlinien absichtlich bezüglich Vorgehensweise und Anwendungsfall sehr unscharf gehalten. Der Weg zur sicheren Maschine oder zum sicheren Produkt soll freigestellt bleiben, nur das Ziel ist festgeschrieben [143]. Die spezieller ausgerichteten EG-Richtlinien zu Brems- und Lenkanlagen [144, 145], insbesondere der dazu gehörige „Elektronikanhang" (Anhang 18 bzw. Anhang 6 der entsprechenden ECE-Regelung), beschäftigen sich mit dem elektronischen Eingriff in die Fahrzeugführung und sind für zukünftige Entwicklungen sehr relevant. Das bei der Typgenehmigung anzuwendende Verfahren, um die Sicherheit von elektronischen Steuersystemen zu gewährleisten, wird hier beschrieben. Um zukünftigen Anforderungen an Lenksysteme, z. B. hinsichtlich Steer-by-Wire, gerecht zu werden, wird die EG-Richtlinie 70/311/EWG [145] respektive 75/321/EWG [146] zurzeit erheblich überarbeitet. Weiterhin befasst man sich auf Basis des „Elektronikanhangs" mit dem Neuentwurf einer ECE-

Regelung, die von Lenkung und Bremse abweichende komplexe elektronische Eingriffe bei Fahrzeugsystemen behandeln soll. Weitere wichtige EG-Richtlinien zur Homologation unterschiedlicher Gruppen von mobilen Arbeitsmaschinen siehe Tabelle 2-1.

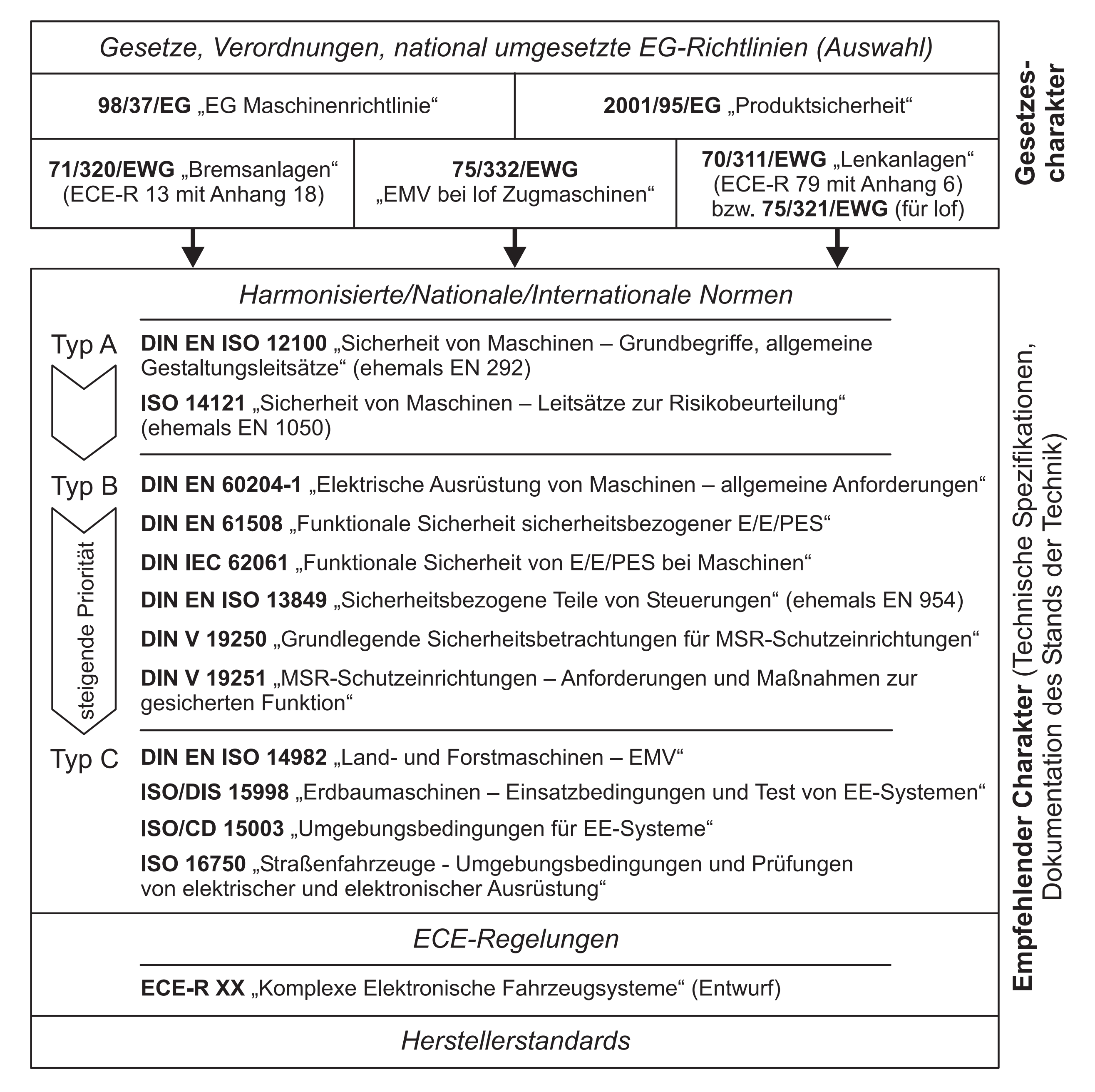


Bild 2-5: *Für die Entwicklung sicherheitsrelevanter Systeme mobiler Maschinensysteme relevante Richtlinien, Normen und Regelungen, Referenzen siehe [141-159].*

Die Norm DIN EN ISO 12100 [147] liegt als allgemeine Grundnorm (Typ A) relativ nahe an der Maschinenrichtlinie und gibt designunabhängige Gestaltungsleitsätze. Hinsichtlich Beurteilung von Gefährdungspotenzial und Risikoanalyse bieten die ISO 14121 [148] und die Standards DIN V 19250, 19251 [149, 150] die nötigen Grundlagen. Sie sind durch eine der umfassendsten Normen zur funktionalen Sicherheit, der EN 61508 [151] referen-

ziert. Der Hauptanspruch dieses Papiers ist die Schaffung einer Grundlage zum Erarbeiten anwendungsbezogener Typ B- und Typ C-Standards für die funktionale Sicherheit von E/E/PE-Systemen. Die IEC 62061 [152] und die ISO 13849 [153] folgen diesem Ziel und konzentrieren sich auf die wesentlichen Aspekte für sicherheitsrelevante Steuerungen bei Maschinen. Der Umfang der EN 61508 wird damit deutlich reduziert, eine unangepasste Anwendung der Papiere auf mobile Arbeitsmaschinen ist aber noch schwierig. Gibt es für Teilsysteme, Fahrzeuggruppen oder spezifische Anwendungen Fachnormen (Typ C), z. B. ISO 14982 „EMV für Land- und Forstmaschinen“ [154], so sind diese in der Anwendung priorisiert. Auch wenn Normen, Regelungen oder Herstellerstandards vor dem Gesetzgeber nicht als bindend erachtet werden, muss im Falle der Produkthaftung eine nach dem Stand der Technik erfolgte Entwicklung der Systeme nachgewiesen werden.

Die besonderen Herausforderungen für funktionssichere Systeme bei mobilen Arbeitsmaschinen entstehen durch

- die Zusammenführung von Arbeitsprozess und Fahrfunktion,
- die Anforderungen schneller Transportfahrt auf öffentlichen Straßen und
- die Vielseitigkeit kombinierbarer Maschinensysteme.

Genau diese Eigenheiten müssen bei der Entwicklung der Systeme sicherheitstechnisch berücksichtigt werden. Ein daran angepasster Entwicklungsleitfaden, basierend auf der richtungweisenden EN 61508 mit Berücksichtigung der anderen Standards aus Bild 2-5 kann dafür die Grundlage bilden.

3 Funktionale Sicherheit als Teil der konstruktiven Sicherheit

Die Vielzahl von verschiedenen Maschinensystemen erschwert eine Standardlösung für die sicherheitsgerechte Entwicklung mobiler Arbeitsmaschinen. Die Anforderungen an die Betriebssicherheit der Systeme differieren untereinander deutlich, was durch das breite Anwendungsspektrum unterschiedlicher Arbeitsprozesse begründet wird. Die geltenden Normen und Richtlinien bieten Hilfe für konstruktive Basislösungen durch konventionelle Sicherheitstechnik (z. B. Absicherung von Quetsch- und Scherstellen) und sind parallel auf den Großteil mobiler Arbeitsmaschinen anwendbar. Die großen Unterschiede und Probleme entstehen dagegen durch neue Entwicklungen hin zu automatisierten Systemen mit verteilter Intelligenz und unterschiedlichsten Überwachungsmaßnahmen hinsichtlich funktionaler Sicherheit, wo wenig standardisierte Vorgehensweisen verfügbar sind.

In diesem Kapitel werden die Maßnahmen funktionaler Sicherheit von der konventionellen Sicherheitstechnik abgegrenzt und die Eigenheiten, auch in Hinblick auf mobile Arbeitsmaschinen, thematisiert. Die grundsätzlichen Möglichkeiten, den sicheren Zustand mit unterschiedlichen Maßnamen der Fehlerbeherrschung zu erreichen, werden aufgezeigt, wobei das Thema Risikominderung unter spezifischen Anforderungen bei mobilen Arbeitsmaschinen behandelt wird.

3.1 Definition der funktionalen Sicherheit

Die Gesamtsicherheit des Systems Mensch/Maschine/Umwelt ist bestimmt durch konstruktive und hinweisende Sicherheit, **Bild 3-1**. Konstruktive Sicherheit erreicht man durch unmittelbare und mittelbare Sicherheitstechnik, sowie durch Maßnahmen funktionaler Sicherheit. Können konstruktive Lösungen potentielle Gefährdungen nicht ausreichend beseitigen, muss durch hinweisende Sicherheitstechnik anhand von Gefahrenhinweisen in der technischen Dokumentation gewarnt werden, siehe auch [141].

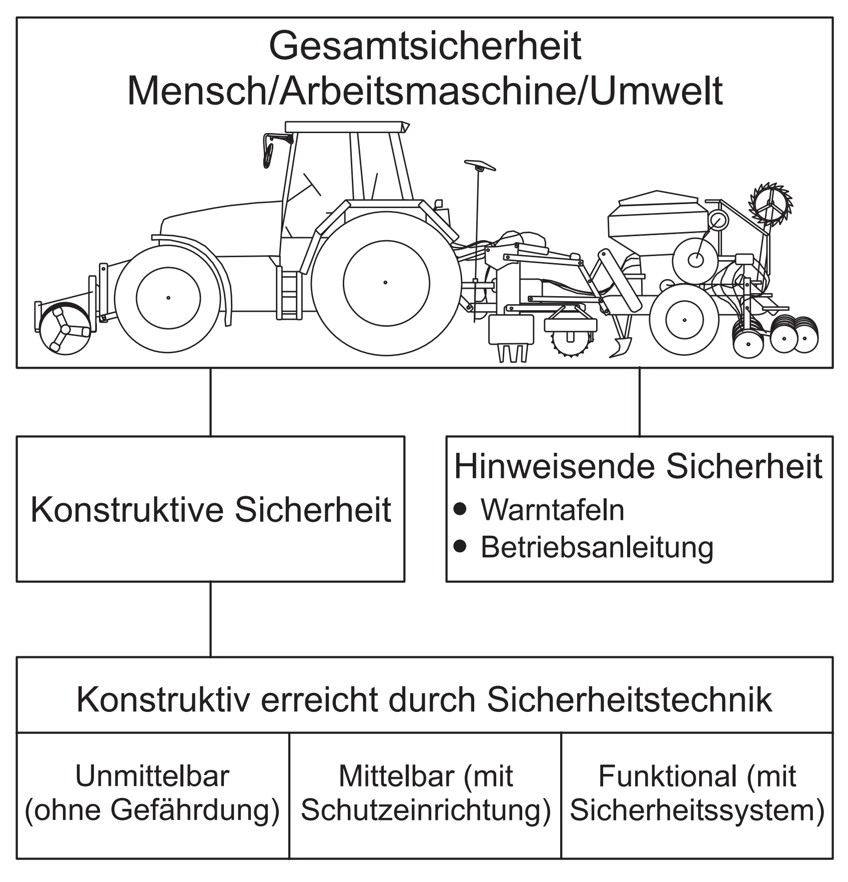


Bild 3-1: *Funktionale Sicherheit komplexer Systeme bei mobilen Arbeitsmaschinen.*

Wichtigster konstruktiver sicherheitstechnischer Leitsatz ist es, die Verwendung von gefährlichen Technologien und Systemlösungen **unmittelbar** zu vermeiden (z. B. Schwachstrom statt Starkstrom). Noch bestehenden Gefährdungen begegnen **mittelbare** Schutzeinrichtungen, so dass Personen von den Gefahrenstellen ferngehalten werden (z. B. Schutzabdeckungen bei Quetsch- und Scherstellen). **Funktionale** Sicherheitssysteme leisten ihren Beitrag zur konstruktiven Sicherheit mit Überwachung der Systeme durch MSR-Sicherheitsfunktionen (Messen, Steuern, Regeln). Sicherheitskritische Fehler müssen dabei rechtzeitig erkannt werden, damit der sichere Zustand durch geeignete Fail-Safe-Strategien erreicht werden kann, bzw. nicht verlassen wird. Die in dieser Arbeit betrachtete funktionale Sicherheit ist laut Normung und Fachwelt definiert als Teil der Gesamtssicherheit eines Systems, der aus der korrekten Funktionalität des MSR-Sicherheitssystems resultiert, welches mit Hilfe durchführbarer Aktionen den sicheren Zustand des Gesamtsystems ansteuert, bzw. aufrechterhält. Dabei kann das Sicherheitssystem intern durch elektrisch/elektronisch/programmierbar elektronische Systeme, auf anderen Technologien basierende Systeme oder auch durch externe Einrichtungen zur Risikominderung realisiert werden [151].

Mittlerweile hat sich der Begriff „funktionale Sicherheit“ als eine zusätzliche Komponente konstruktiver Sicherheit durchgesetzt. Die funktionale Sicherheit mechatronischer Systeme mobiler Arbeitsmaschinen gliedert sich anwendungsbezogen in die beiden Hauptbereiche:

- Sicherheit elektronischer Eingriffe in die Fahrzeugführung (Fahrsicherheit durch Assistenzsysteme, aktive Sicherheitssysteme, u. U. basierend auf X-by-Wire-Technologie).

- Sicherheit automatisierter und elektronisch geregelter Arbeitsprozesse (Prozesssicherheit, Automatisierungstechnik).

Grundlegende Themenstellung des zu Beginn angesprochenen DFG-Projekts war der hier zweitgenannte Punkt, nämlich die Prozesssicherheit elektronisch geregelter, automatisierter Systeme.

3.2 Maßnahmen zur Gewährleistung des sicheren Zustands

Die VDI-Richtlinie VDI/VDE 3542 [160] definiert den **sicheren Zustand** als Zustand eines technischen Systems, bei dem aufgrund der getroffenen Schutzmaßnahmen gegen mögliche sicherheitsbezogene Fehlfunktionen das Risiko vertretbar gering ist. Bei der Konzeption der MSR-Sicherheitsfunktionen müssen die genauen Merkmale des sicheren Zustands vorher konkret festgelegt werden. Grundsätzlich gibt es zwei verschiedene in **Bild 3-2** dargestellte Wege der Fehlerbeherrschung, den sicheren Zustand eines Systems zu erreichen und damit der Fail-Safe-Anforderung im Fehlerfall zu genügen.

Das System mit **Fail-Silent**-Verhalten wird unmittelbar nach Erkennen einer Fehlfunktion abgeschaltet. Dabei muss sichergestellt sein, dass das Abschalten der Funktion keine kritischen Systemzustände herbeiführt. Beispiel hierfür ist das Deaktivieren eines fehlerhaften ABS-Systems im Kfz, wobei der Fahrer durch eine Fehlermeldung über den Ausfall des Systems in Kenntnis gesetzt, die Hauptfunktionalität der Bremse dadurch aber nicht beeinträchtigt wird. Bei erkennbarem Ausfall werden durch diese Systeme die Weitergabe falscher Daten bzw. fehlerhafte Eingriffe für das Gesamtsystem verhindert. Fail-Silent-Systeme werden deshalb auch als **integere** Systeme bezeichnet.

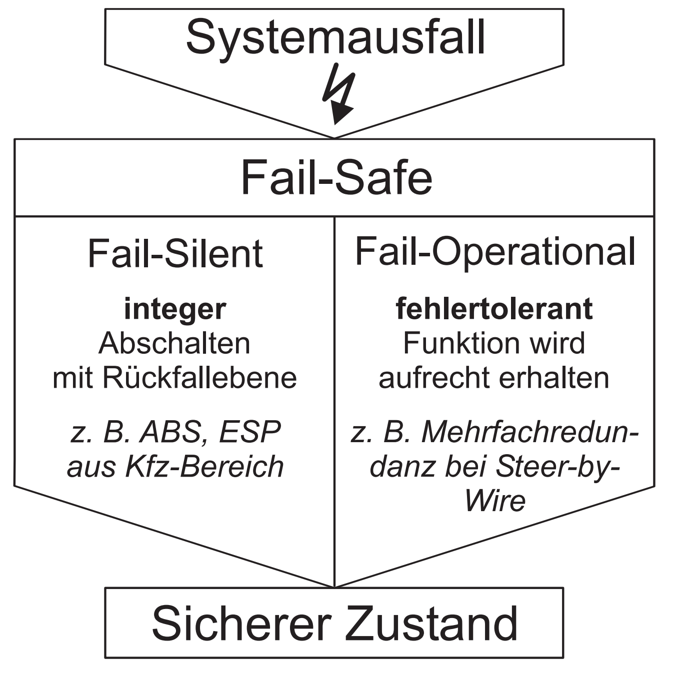


Bild 3-2: *Erreichen des sicheren Zustands durch unterschiedliche Fail-Safe-Strategien nach einem Fehlerfall.*

Systeme mit **Fail-Operational**-Verhalten müssen **fehlertolerant** ausgelegt sein, d. h. das System hält nach Erkennen einer Fehlfunktion seine Funktionalität voll aufrecht. Fehlertoleranz liegt vor, wenn die durch die externe Systemspezifikation festgelegten Anwendungsfunktionen auch dann ausfallfrei bleiben, wenn in einzelnen Komponenten Fehler

im Rahmen der Fehlervorgabe, die die Menge der zu tolerierenden Fehler anhand eines Fehlermodells beschreibt, auftreten [161]. Denkbare Beispiele hierfür sind mehrkanalig (redundant) ausgeführte elektronische Lenksysteme (Steer-by-Wire). Hier muss das System auch nach Ausfall eines Kanals durch Einspringen eines zweiten bzw. n-ten Kanals redundant verfügbar bleiben.

Zeitverhalten fehlerbeherrschender Maßnahmen

Die zentrale Voraussetzung zur Fehlerbeherrschung in beiden dargestellten Abstufungen ist das Erkennen sicherheitskritischer Fehler innerhalb einer für das System angemessenen Fehlertoleranzzeit, definiert als Zeit zwischen Auftreten des eigentlichen Fehlers und dem Zeitpunkt, an dem das System seinen bestimmungsmäßigen Betrieb verlässt und in den kritischen Zustand übergeht. Die Zeit, die verstreicht, den Fehler eindeutig zu diagnostizieren und die darauf folgende Fehlerreaktionszeit des MSR-Sicherheitssystems müssen als Summe unterhalb der Fehlertoleranzzeit liegen, **Bild 3-3**.

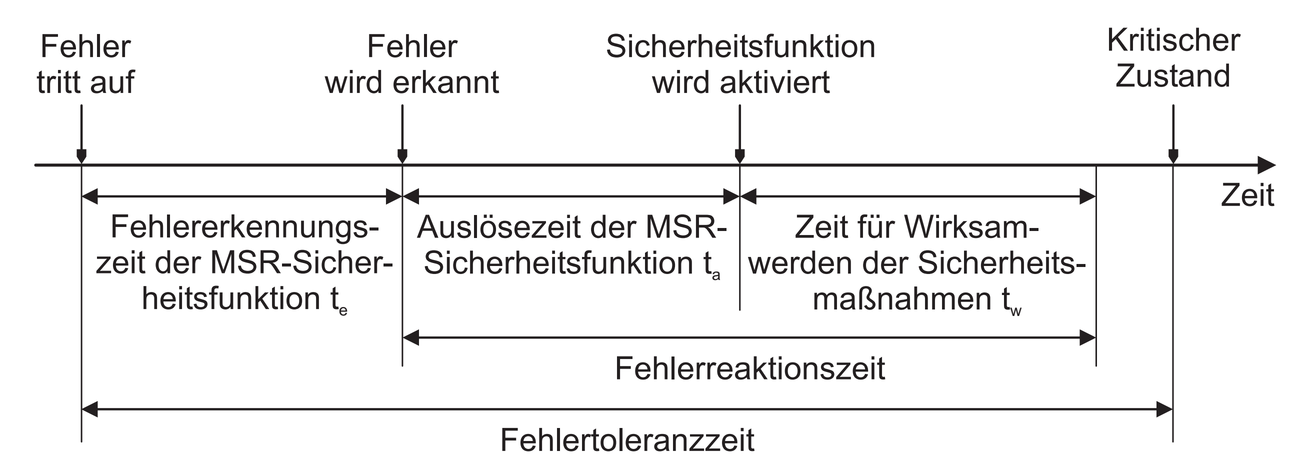


***Bild 3-3:** Zeitverhalten von integeren oder fehlertoleranten MSR-Sicherheitsfunktionen, abhängig von der Fehlertoleranzzeit (Zeit vom Auftreten des Fehlers bis zum kritischen Zustand) in Anlehnung an [150].*

3.3 Risikominderung bei mobilen Arbeitsmaschinen

Die Sicherheit eines Maschinensystems wird häufig durch das Risiko bestimmter Systemausfälle oder -fehlfunktionen beschrieben. Der Begriff „Risiko“ wird dabei als Verknüpfung der Wahrscheinlichkeit für das Auftreten eines bestimmten Fehlers mit der daraus resultierenden Schadensschwere verstanden. Bei der Entwicklung einer Maschine oder eines Maschinensystems muss das Gefährdungspotenzial sicherheitskritischer Funktionen bestimmt und die notwendigen Minderungen der Teilrisiken daraus abgeleitet werden. Eine Methode der quantitativen Risikobestimmung für eine spezielle Schutzmaßnahme ist die im Kapitel 4.2.1.2 beschriebene Risikoanalyse, eine Klassifizierungsmethode für das

Sicherheitsrisiko charakterisiert nach Schadensschwere und Auftretenswahrscheinlichkeit des Fehlers.

Um erforderliche Risikominderungen zu bewerkstelligen, stehen unterschiedliche Maßnahmen zur Verfügung, siehe **Bild 3-4**. Durch das Zusammenwirken konstruktiver und hinweisender sicherheitstechnischer Maßnahmen sowie externer Maßnahmen (z. B. die weiträumige Absperrung des Gefahrenbereichs) wird das Gesamtrisiko auf einen notwendigen Level reduziert. Das Niveau des akzeptablen Risikos einer Schutzmaßnahme kann abhängig von der Risikoklasse durch Schwellwerte für real berechnete Ausfallwahrscheinlichkeiten oder eine dem Risiko angepassten Entwicklungsmethodik nachgewiesen werden. Aufgabe eines sicherheitsgerichteten Entwicklungskonzepts sind Festlegung einer angemessenen Systemarchitektur, Bestimmung der Höhe der notwendigen Risikominderungen und Aufzeigen systematischer bzw. methodischer Möglichkeiten, die geforderte Risikominderung zu realisieren. Das nach allen getroffenen Maßnahmen zur Risikominderung bestehende vertretbare Risiko bleibt als Restrisiko bestehen.

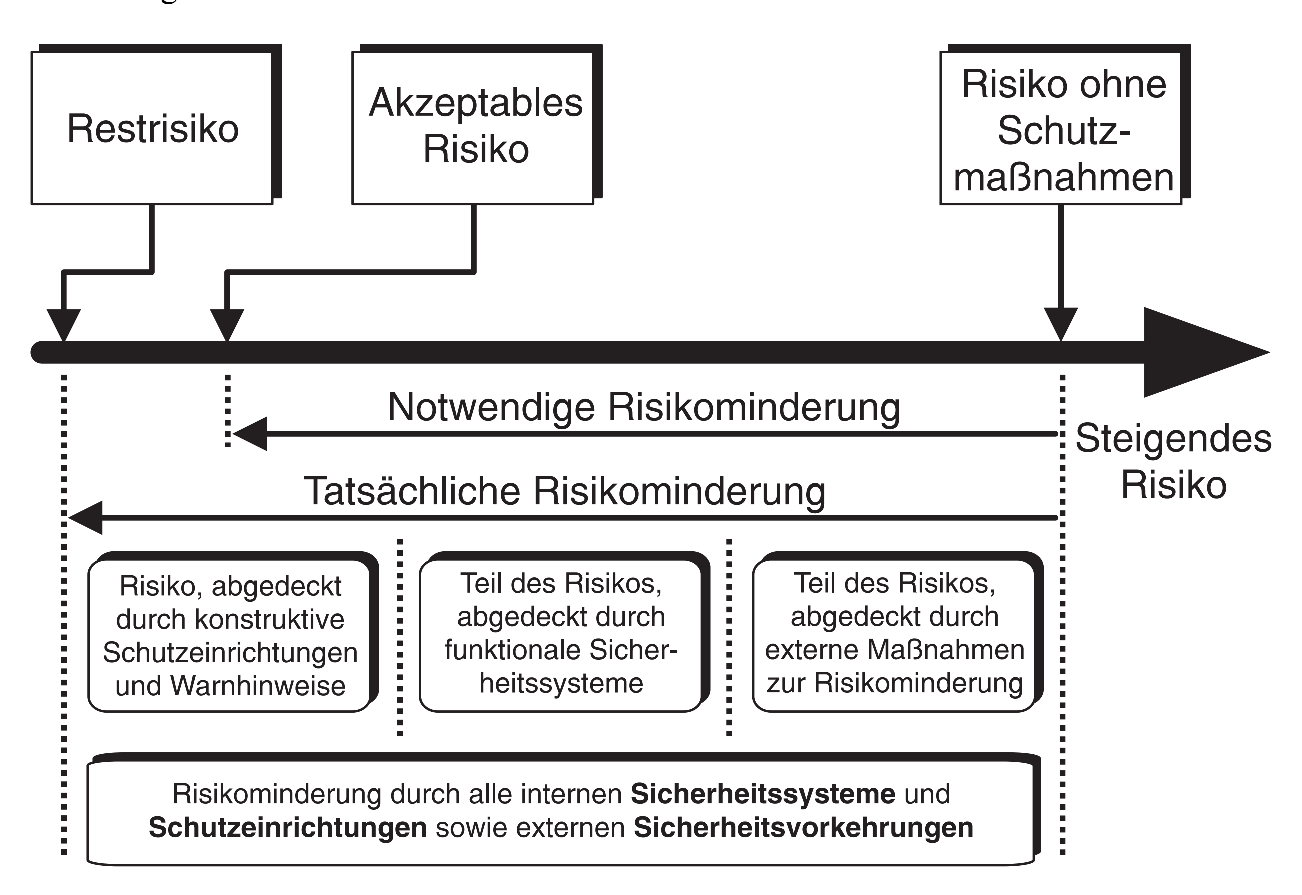


Bild 3-4: *Risikominderung für ein mechatronisches System durch Maßnahmen konstruktiver und hinweisender Sicherheitstechnik, insbesondere funktionaler Sicherheit, und externe Maßnahmen.*

Resultierend aus den in Kapitel 2.1 beschriebenen Charakteristika mobiler Arbeitsmaschinen entstehen hohe Anforderungen an funktionale Sicherheitsmaßnahmen zur Risikominderung der Systeme. Gründe dafür sind beispielsweise

- hohe Komplexität der Automatisierungen durch Koordination von Prozessregelung und Fahrfunktion,
- Variantenvielfalt der Leistungsschnittstellen mit unterschiedlichen Technologien (Mechanik, Hydraulik, Elektrik, Pneumatik),
- Gesamtfunktionalität realisiert durch verteilte Systeme (Anzahl der elektronischen Steuergeräte, Datenkommunikation, Plug-and-Play-Funktionalität zwischen Hauptmaschine und Gerät),
- steigende Transportgeschwindigkeiten auf öffentlichen Straßen (StVZO).

Die Anforderungen können durch unterschiedliche Überwachungsstrategien und Sicherheitskonzepte erfüllt werden. So überwachen z. B. Plausibilisierungen von Systemparametern und Kontrollen gültiger Messwertbereiche die sicherheitsrelevanten Prozessgrößen. Mechanische Bewegungsabläufe werden automatisch zueinander koordiniert, z. B. Bewegungen zwischen Hauptmaschine und Gerät, und elektronische Anschläge verhindern Kollisionen.

4 Entwicklungsmethoden

Nach Ehrlenspiel unterscheidet man sachgebundene Entwicklungsmethoden, ausgerichtet auf das Erreichen eines vorgegebenen, sachlichen Ziels, z. B. eines Dokuments oder Objekts, und Organisiationsmethoden, deren Ziel die Gestaltung eines Entwicklungsprozesses oder Handlungssystems ist [162]. Die in diesem Kapitel behandelten Entwicklungsmethoden haben alle fest vorgegebene Objektziele, wie z. B. die Ermittlung eines Risikopotenzials, Abbildung der Systemstruktur oder Verbesserung der Zuverlässigkeit eines Systems. Sie sind damit sachgebundene Methoden, die in ein übergeordnetes Entwicklungsmodell, z. B. nach Kapitel 5.2, eingebettet werden. Für die Realisierung der vorgestellten Entwicklungsvorgänge im Unternehmen empfehlen sich zusätzlich organisationsgebundene Methoden im Rahmen eines integrierten Vorgehens. Bei Durchführung der Forschungsarbeiten wurden auch diese soweit möglich angewandt. Für weitergehende Informationen zu organisationsgebundenen Methoden sei auf [162] verwiesen.

In diesem Kapitel werden geeignete Methoden für die Entwicklung von elektronischen Systemen bei mobilen Arbeitsmaschinen vorgestellt, die im Rahmen der Forschungsarbeiten erprobt, teilweise weiterentwickelt und an den Anwendungsfall angepasst wurden. Die Entwicklungsmethoden teilen sich dabei in sachgebundene Methoden mit **konventioneller** und **modellbasierter** Vorgehensweise auf. Im Gegensatz zu konventionellen Methoden liegt die gemeinsame Strategie modellbasierter Methoden darin, Maschinensysteme und Reglerstrukturen in Simulationen am Rechner zu modellieren und in den einzelnen Schritten innerhalb der Softwareentwicklung miteinander effektiv zu verknüpfen. Die aufgestellten Reglermodelle werden anhand der simulierten Strecke wie auch im realen Anwendungsfall spezifiziert, entwickelt, getestet und für den endgültig implementierten Regler im Seriensteuergerät weiterverwendet.

4.1 Überblick über mögliche Methoden

Für die sicherheitsgerechte Entwicklung programmierbar elektronischer Systeme steht eine Vielzahl an unterschiedlichen Methoden und Maßnahmen zur Verfügung. **Tabelle 4-1** soll Überblick und Entscheidungshilfe für die Auswahl geeigneter Methoden bieten und bei der Zuordnung zu einzelnen Entwicklungsschritten helfen. Sie dient u. a. als Leitfaden für die folgenden Unterkapitel. Die aufgeführten Entwicklungsmaßnahmen sind grob in die Phasen Spezifikation sowie Test/Validierung konform zur linken und rechten Seite des V-Modells unterteilt, vergleiche Bild 2-4. Zusätzlich sind die angesprochenen Detaillierungsebenen (System-, Modul- oder Komponentenebene) aufgeführt, um eine vertikale Einordnung in das V-Modell zu ermöglichen. In den letzten beiden Spalten der Tabelle wird erklärt, ob die Methode oder Maßnahme bei den Entwicklungen des Anwendungsbeispiels der vorliegenden Arbeit verwendet und/oder weiterentwickelt wurde.

4.2 Konventionelle Methoden für die Systementwicklung

Bei der Entwicklungsarbeit läuft der normale Ablauf des Denken und Handelns größtenteils **implizit** ab, d. h. unter automatischer Verwendung konventioneller Methoden im Hintergrund, ohne sich einer speziellen Methodenwahl bewusst zu sein. Die hier angesprochenen **expliziten** Methoden beziehen sich auf ein vorher definiertes Ergebnis mit Festschreibung in Formularen, Dokumenten oder digitalen Daten und werden den einzelnen Schritten des V-Modells zugeordnet. Methoden mit konventioneller Vorgehensweise sind alle üblichen Methoden, die **nicht** modellbasiert im Sinne von Kapitel 4.3 aufgebaut sind. Sie begleiten die Entwicklung von Systemkomponenten (Software und Hardware) sowie übergeordneten mechatronischen (Teil-)Systemen.

4.2.1 Methoden zur Spezifikation und Systemauslegung

4.2.1.1 Systemstrukturanalyse

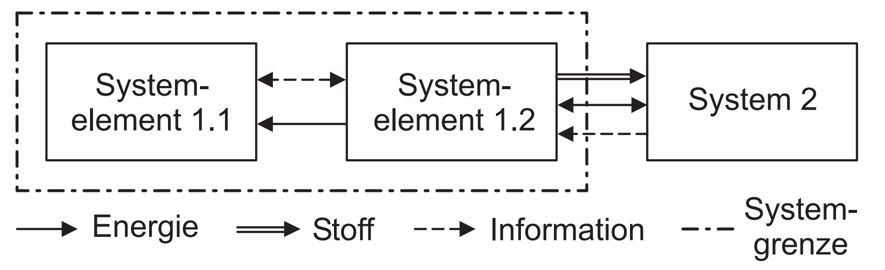


Bild 4-1: *Allgemeiner Signalflussplan zweier Systeme mit Energie-, Stoff- und Informationsflüssen.*

In den ersten Schritten der Spezifikationsphase können die allgemeinen Systemfunktionen mit Hilfe der Systemstrukturanalyse aus den Anforderungen entwickelt und in Funktionsgruppen und -modulen mit Hilfe eines Signalflussplans (**Bild 4-1**) angeordnet werden. Die Black-Box-

Tabelle 4-1: *Entwicklungsmethoden für die Elektronikentwicklung (eine Auswahl).*

Methode/Maßnahme	Spezifikation	Test/Validierung	Systemebene	Modulebene	Komponentenebene	modellbasiert	konventionell	Simulation	HW-bezogen	SW-bezogen	systembezogen	weiterentwickelt	verwendet
Modellbasierte Spezifikation	x		x			x			x	x	x		
Lastenheft/Anforderungsanalyse	x		x				x		x	x	x		x
Systemstrukturanalyse	x		x	x			x		x		x	x	x
Risikoanalyse	x		x	x			x				x	x	x
System-FMEA	x		x	x			x		x		x	x	x
Fehlerbaumanalyse	x		x	x	x		x		x		x		x
Strukturierte Analyse	x				x		x			x			x
Model-in-the-Loop	x			x		x		x	x	x	x	(x)	x
Rapid-Control-Prototyping	x			x	x	x		x	(x)	x	(x)	(x)	x
Komponenten-FMEA	x				x		x		x			x	(x)
Automat. Code Generierung	x			(x)	x	x				x			
Software-Criticality-Analysis	x			x	x		x			x			
erprobte Hardware	x				x		x		x				x
SW-Standards	x				x		x			x			x
SW-Konfigurationsmanagement	x			(x)	x	(x)	x			x			x
SW-Audit	x			(x)	x		x			x			
SW-Debuggen		x			x		x			x			x
EEPROM-Simulation		x			x		x	x		x			x
SW-Performance-Test		x			x	(x)	x		x	x			
Komponententests		x			x		x	(x)	x	x			
Software-in-the-Loop		x		x	x	x		x		x			(x)
Hardware-in-the-Loop		x		x		x		x	x	x		(x)	x
Statische Software-Analyse		x		x	x		x			x			x
Dynamische Softwaretests		x		x	x		x			x			x
ECU-Labortest		x		x		(x)	x	x	x	x			x
EMV-, Umwelt-, Vibrationstests		x		x	x		x		x		x		(x)
Simulation auf dem Prüfstand		x	x	x			x	x	x	x	x		x
Worst-Case-Szenarios		x	x				x		x	x	x		x
Test der Funktionalität		x	x	x			x		x	x	x		x
Test des Fehlerverhaltens		x	x	x			x		x	x	x		x
Systemtest		x	x	x			x				x		x
Test im breiten Anwendungsfeld		x	x				x				x		

x: trifft zu, (x): trifft bedingt zu

Darstellung mit den Umsatzarten Energie, Stoff und Information erleichtert dabei die Definition der Schnittstellen. Das Bild zeigt ein allgemeines Anschauungsbeispiel.

4.2.1.2 Bestimmung des Gefährdungspotenzials durch Risikoanalyse

Grundlage für die Bestimmung des Risikopotenzials eines Maschinensystems ist die Untersuchung der einzelnen, als sicherheitsrelevant eingestuften Teilsysteme mit der Methode Risikoanalyse, wie sie in den Vornormen DIN V 19250 [149] und 19251 [150] beschrieben ist. Das Vorgehen orientiert sich am so genannten Risikographen, der eine quantitative Einteilung des jeweiligen Teilsystems in unterschiedliche Integritätsklassen erlaubt, **Bild 4-2**. Der hier gezeigte Graph wurde an die Anwendungsfälle für mobile Arbeitsmaschinen hinsichtlich relevanter Schadensklassen und weiterreichende Eingriffsmöglichkeiten des Fahrers angepasst.

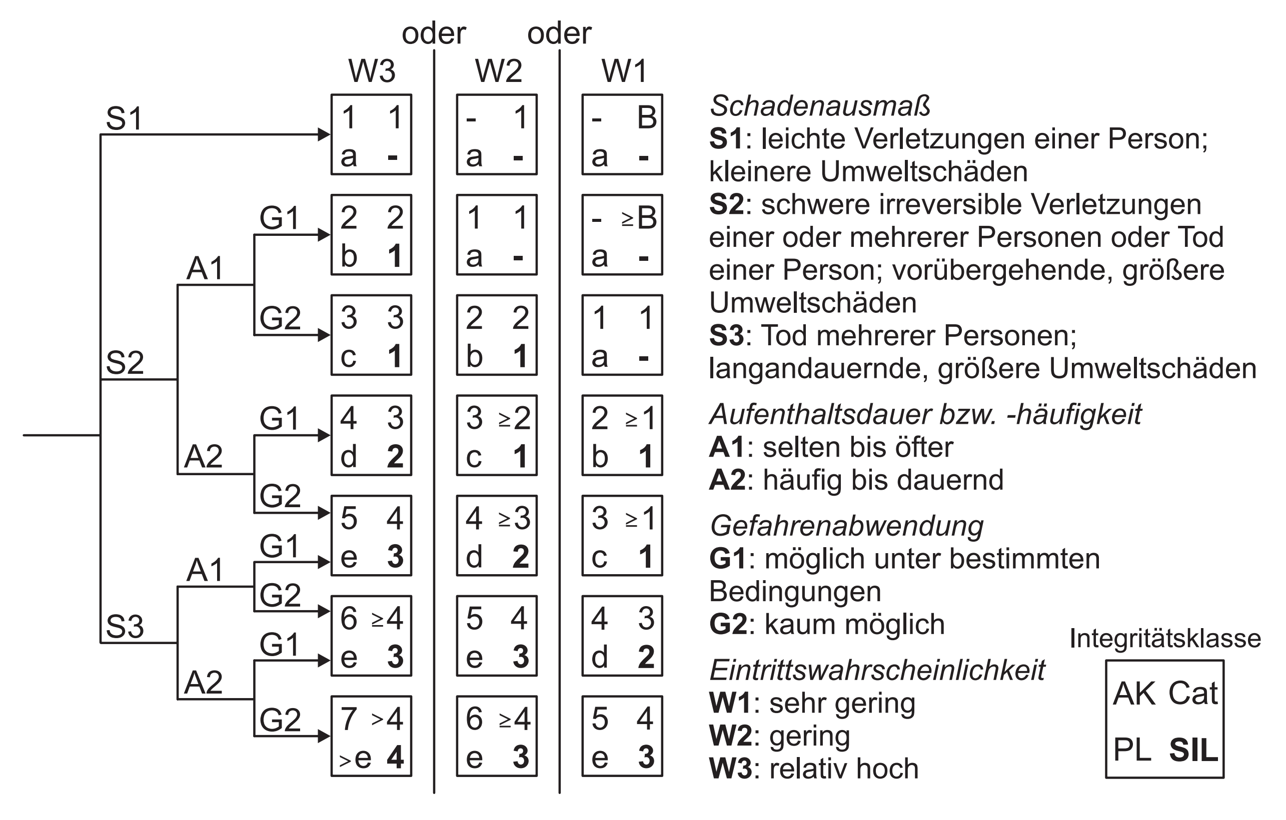


Bild 4-2: *Angepasster Risikograph zur Bestimmung der sicherheitstechnischen Anforderungen einer einzelnen MSR-Sicherheitsfunktion in Anlehnung an [149, 150]. Ergebnis sind die je nach Norm spezifizierten Integritätsklassen (Kästchen). Für eine weitere Verwendung wurde der Safety-Integrity-Level SIL nach EN 61508 favorisiert,* ***Tabelle 4-2****.*

Wichtig ist die Bearbeitung des Gesamtsystems in mehreren Risikoanalysen, unterteilt nach Teilsystemen bzw. MSR-Sicherheitsfunktionen. Beim Durchlaufen des Graphs von links nach rechts wird die behandelte MSR-Sicherheitsfunktion nach den Kriterien

- Schadenausmaß (S)

- Aufenthaltsdauer bzw. -häufigkeit (A)
- Gefahrenabwendung (G) und
- Eintrittswahrscheinlichkeit (W)

für das unerwünschte Ereignis bewertet. Im Folgenden sollen die Integritätsklassen erläutert sowie die wichtigsten Eigenschaften der Kriterien S bis W aufgezeigt werden.

Tabelle 4-2: *In der Normung verwandte, unterschiedliche Begriffe für erforderliche Integritätsklassen.*

Norm	Bezeichnung/Begriff
EN 61508 [152]	Safety-Integrity-Level (SIL)
ISO 13849 [153]	Performance Level (PL)
DIN V 19250, 19251 [149, 150]	Anforderungsklasse (AK)
EN 954 [163]	Kategorie (Cat)

Die Integritätsklasse eines Sicherheitssystems und damit das Ergebnis der Risikoanalyse bestimmt die Fähigkeit, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen korrekt auszuführen. Die sicherheitstechnischen Anforderungen hinsichtlich Entwicklungsprozess und Auslegung der MSR-Sicherheitsfunktionen werden so festgelegt, um die notwendige Risikominderung zu erfüllen. In den gängigen Sicherheitsnormen werden verschiedene Bezeichnungen für die resultierenden Integritätsklassen verwendet, siehe Tabelle 4-2. Mittlerweile hat sich die Integritätsklasseneinteilung der EN 61508 [152] mit unterschiedlichen Safety-Integrity-Levels (SIL) von SIL1 bis SIL4 als diskretes Maß der Zuverlässigkeit bzw. sicherheitstechnischen Verantwortung eines Systems durchgesetzt und bildet auch für vorliegende Arbeit die Grundlage.

Schadenausmaß S

Durch die Baumstruktur des Risikographs legt die Bestimmung des Schadenausmaßes schon im ersten Schritt der Untersuchung den groben Bereich des resultierenden SIL fest und hat damit das größte Gewicht. Die Norm weist ausdrücklich darauf hin, dass bei Bewertung von S die im Regelfall zu erwartenden Unfallfolgen und üblichen Heilungsprozesse vorausgesetzt werden sollen. Um eine ehrliche und möglichst objektive Ermittlung des SIL zu gewährleisten, ist es wichtig, diesen Grundsatz zu beachten und bei der Bewertung des Schadenausmaßes nicht in extreme Szenarios zu fallen.

In durchgeführten Risikoanalysen aus den Bereichen mobiler Arbeitsmaschinen und Kfz hat es sich gezeigt, dass das Schadenausmaß S3 auf keinen Fall überschritten wird, was mit Beschränkung der Schadensklassen von S1 bis S3 bei Anpassung des Risikographs berücksichtigt wurde. Beispiele für S3 sind gravierende Auswirkungen durch Unfälle von Gefahrguttransporten oder Omnibussen zur Personenbeförderung. Das Schadenausmaß S2 ist für die meisten sicherheitskritischen Systeme mobiler Arbeitsmaschinen ausreichend.

Aufenthaltsdauer bzw. -häufigkeit A

Mit diesem Kriterium wird der Aufenthalt von Personen im Gefahrenbereich hinsichtlich zeitlicher Dauer und Häufigkeit spezifiziert. Im Unterschied zu stationären Maschinen ist bei mobilen Arbeitsmaschinen zu berücksichtigen, dass sich das Umfeld der Maschine oftmals ändert. Es muss deshalb von zwei zu verknüpfenden Aufenthaltshäufigkeiten ausgegangen werden:

1. Potenzielle Gefährdung aus der Situation „Maschine in veränderlicher Umgebung". Die Aufenthaltshäufigkeit der Maschine in potenziellen Gefährdungsbereichen in der Umwelt ist maßgeblich (z. B. Transportfahrt im Stadtverkehr).
2. Potenzielle Gefährdung aus der Situation „Mensch im Aktionsbereich der Maschine". Die Aufenthaltshäufigkeit für Personen in Gefahrenbereichen der Maschine ist maßgeblich (z. B. zusätzliches Bedienpersonal oder Fußgänger).

Gefahrenabwendung G

Die Möglichkeiten zur Gefahrenabwendung sind von unterschiedlichen Faktoren abhängig. Der zeitliche Entwicklungsverlauf des Gefahrenzustandes, ob plötzlich oder stetig langsam, muss genauso in die Bewertung miteinfließen wie die Möglichkeit zur Abwendung der Gefahr durch potenzielle Fluchtmöglichkeiten oder Abschalten des Systems (Fail-Silent), wenn dazu genügend Zeit besteht. Steht ein Arbeitsprozess unter ständiger Kontrolle von technisch versiertem Fachpersonal und liegt der notwendige Eingriff in die Maschinenführung im Bereich einer natürlichen Reaktion, so kann ein Fehler möglicherweise rechtzeitig erkannt und das unerwünschte Ereignis abgewendet werden. Da die Arbeitsprozesse und Transportfahrten mobiler Arbeitsmaschinen grundsätzlich von einem geschulten Fahrer überwacht werden, wurde die Möglichkeit zur Gefahrenabwendung im Risikographen zusätzlich bei S3 berücksichtigt, was in der ursprünglichen Fassung ausgeschlossen war.

Eintrittswahrscheinlichkeit W des unerwünschten Ereignisses

Mit diesem Parameter wird die Eintrittswahrscheinlichkeit des unerwünschten Ereignisses **ohne** Vorhandensein der MSR-Sicherheitsfunktion beurteilt. Unter Berücksichtigung der **Betriebsbewährtheit** wird eine Aussage darüber getroffen, wie viele Unfälle unter gegebenen Umständen zu erwarten sind. Fehlen statistische Erfahrenswerte für die Eintrittswahrscheinlichkeit eines Fehlers, empfiehlt es sich gerade bei diesem Parameter, die Situation im Zweifel schärfer zu beurteilen. Im Bereich innovativer, elektronisch geregelter Automatiken bei mobilen Arbeitsmaschinen gelangt man daher oft in hohe Eintretenswahrscheinlichkeiten. Bewertungen von W2 und W3 herrschen vor.

Bestimmung der Integritätsklassen mit dem Risikographen

Beim Verfolgen des gewählten Pfades im Risikographen von links nach rechts ergeben sich als Endergebnis unter Berücksichtigung der Eintrittswahrscheinlichkeit einige Felder für Integritätsklassen, für die auf besondere, u. U. über den Stand der Technik hinausgehende, sicherheitstechnische Maßnahmen verzichtet werden kann (nicht belegte Felder, bzw. Basisanforderungen für Cat B). In allen übrigen Fällen bestimmt der entsprechende SIL den Umfang der MSR-Sicherheitsfunktion. Zum Beispiel führt die Risikoanalyse der Überwachungseinheit eines ABS-Systems über den Pfad S2, A2, G2 und W2 zu einem Safety-Integrity-Level SIL2, was als Konsequenz eine Fail-Silent-Charakteristik des Systems erforderlich macht. Weitere Beispiele für Einstufungen von E/E/PE-Systemen nach dem Risikographen ist SIL3 für fehlertolerant ausgeführte Steer-by-Wire-Systeme oder SIL 1 für elektronische Komfortsysteme für Fensterheber oder Scheibenwischer.

Die Risikoanalyse verfolgt als Schwerpunkt die Beurteilung einer Gefahrensituation, die durch Nichtvorhandensein oder fehlerhaftes Verhalten einer MSR-Sicherheitsfunktion entsteht. Die Anforderungen daraus können als notwendige Absicherung z. B. eine Fehlermöglichkeits- und -einflussanalyse (FMEA) [164] auf System- und/oder Komponentenebene im frühen Stadium der Systementwicklung erfordern.

4.2.1.3 System-FMEA nach VDA 4.2

Die Fehlermöglichkeits- und -einflussanalyse (FMEA) ist eine Methode dafür, potenzielle Fehlerfälle aufzudecken, Ursachen und Folgen der Fehler abzuleiten und den Fehler nach seinem Risiko zu klassifizieren. Die Methode stammt ursprünglich aus den USA, wo sie von der NASA zur systematischen Absicherung der APOLLO-Projekte eingesetzt wurde [165]. Mittlerweile ist sie ein fest etabliertes Werkzeug der qualitäts- und sicherheitsgerichteten Produktentwicklung – nicht nur für den Automotive-Bereich. Die Methodik wird mittlerweile fast ausschließlich durch Softwarelösungen und Rechneranwendung unterstützt. Die FMEA-Werkzeuge reichen von Vorlagen für einfache Tabellen-FMEA bis zu spezialisierten Anwendungen zur Systemanalyse, wie z. B. Tools der Fa. PLATO [166] und das für diese Arbeit verwendete Risk RM der Fa. APIS [167]. Diese Werkzeuge erleichtern die systematische Vorgehensweise und bieten schlüssige Datenbankkonzepte zur Weiterverwendung einmal aufgestellter Teiluntersuchungen.

Methodische Grundsätze

Grundsätzlich unterscheidet man die FMEA in drei verschiedenen Arten, Konstruktions-FMEA, Prozess-FMEA und System-FMEA. Die **Konstruktions-FMEA** untersucht die im Pflichtenheft festgelegten Merkmale eines Produktes während der Entwicklungsphase. Mit Hilfe einer reinen Tabellen-FMEA wird das Produkt vorwiegend auf Bauteil- und Baugruppenebene hinsichtlich des hineinkonstruierten Risikos untersucht.

Die **Prozess-FMEA** baut auf den Ergebnissen der Konstruktions-FMEA auf. Sie untersucht den Herstellungsprozess auf die Eignung zur Herstellung der geforderten Produkteigenschaften. Die einzelnen Prozessschritte des Gesamtprozesses werden auf ein fertigungstechnisches Risiko untersucht.

Die Haupt-Nachteile von konventioneller Konstruktions- und Prozess-FMEA sind:

- Nichterfassung der funktionalen Zusammenhänge
- Unzureichende Dokumentation in der reinen Tabellen-FMEA
- Schwierige Fokussierung auf den zu untersuchenden Detaillierungsgrad

Um diese Nachteile zu beseitigen, wurde die Methode zur **System-FMEA** mit methodischer, systematischer Vorgehensweise weiterentwickelt und im Leitfaden VDA 4, Teil 2 [164] standardisiert. Bei der System-FMEA wird das gesamte Produkt bzw. der gesamte Prozess als Zusammenschluss logisch vernetzter Teilsysteme bzw. Prozessschritte betrachtet. Die systematische Methodik erleichtert es dabei, den festgelegten Detaillierungsgrad nicht zu überschreiten und die zu untersuchenden Systeme trotzdem komplett abzuarbeiten. Die System-FMEA „Produkt" untersucht Funktionsfehler von Teilsystemen und die daraus resultierenden Ausfallfolgen auf das Gesamtsystem. Die System-FMEA „Prozess" behandelt die Prozessschritte eines Arbeitsprozesses anhand der Einflussgrößen Mensch, Maschine, Methode, Material und Mitwelt (die so genannten 5 Ms). Ergebnisse aus der System-FMEA können es erfordern, Teilsysteme in untergeordneten Teil-FMEA, bzw. einzelne Bauteile oder Prozessschritte in Komponenten-FMEA eingehender zu untersuchen.

Zur Analyse von automatisierten Arbeitsprozessen bei mobilen Arbeitsmaschinen hat sich eine Kombination aus System-FMEA „Produkt" und „Prozess" mit Beachtung folgender methodischer Grundsätze bewährt:

- Präventive Anwendung in einer frühen Phase der Entwicklung bzw. Auslegung des automatisierten Arbeitsprozesses im Zusammenspiel mit der Risikoanalyse (siehe zuvor).
- Durchführung der Analyse in interdisziplinärer Teamarbeit mit Mitarbeitern aus den Bereichen Entwicklung, Versuch, Elektronik, Qualitätsmanagement und Kundendienst.
- Systematische Vorgehensweise nach VDA 4.2 (siehe unten).
- Kombination der Teilsysteme, ihrer zu erledigenden Teilprozesse und der notwendigen Einflussgrößen bei der Strukturanalyse des Systems.
- Ergebnisdokumentation durch die Verwendung von Systembäumen, Funktionsbäumen, Fehlerbäumen, Formblättern und Bewertungskatalogen.

Die fünf Schritte der System-FMEA

Bei Durchführung einer FMEA schlägt der VDA eine systematische Vorgehensweise in den fünf Schritten Strukturanalyse, Funktionsanalyse, Fehleranalyse, Risikobewertung und Maßnahmenoptimierung vor, welche im Folgenden beschrieben sind, **Bild 4-3**.

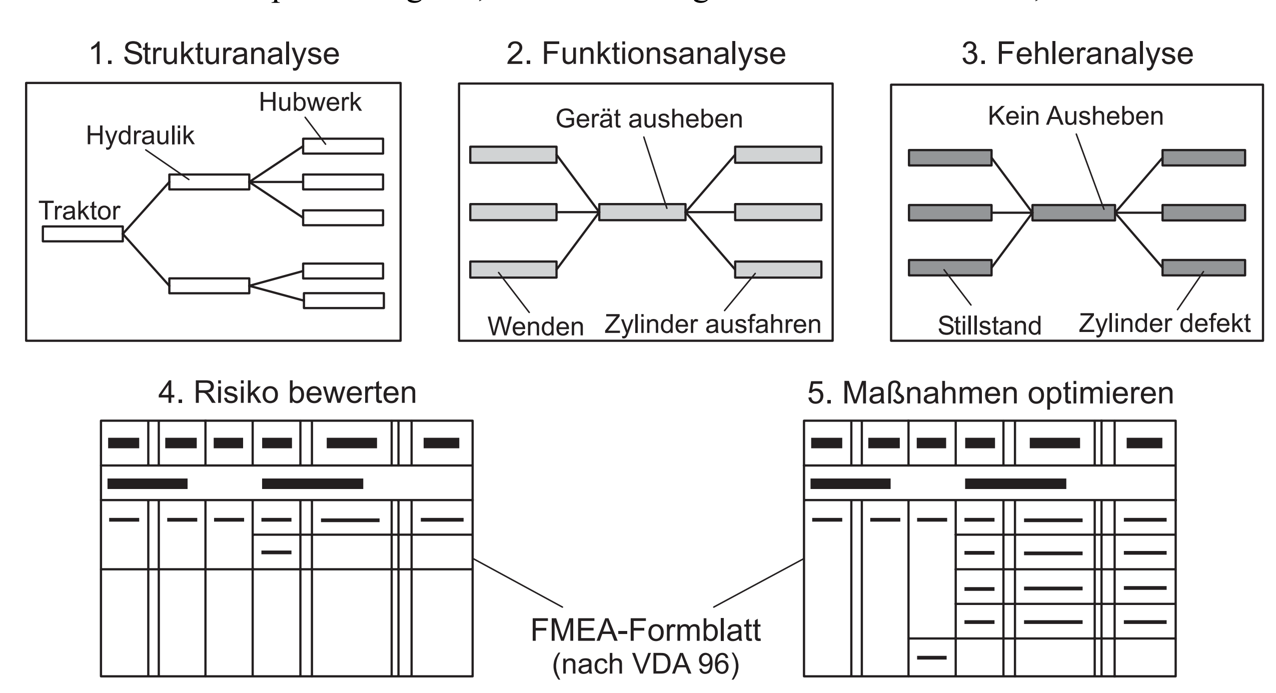


Bild 4-3: *Die fünf Schritte der System-FMEA nach VDA 4 Teil 2.*

Im ersten Schritt, der **Strukturanalyse**, wird das Gesamtsystem in die einzelnen Teilsysteme bis hin zu den einzelnen Systemelementen der Teilsysteme strukturiert. Ähnlich einer Stückliste entsteht dadurch ein Systembaum in der Top-Down-Analyse. Bei Untersuchung eines Arbeitsprozesses wird der Prozess in die einzelnen Teilprozesse bzw. Prozessschritte aufgeteilt und in der untersten Ebene durch die beteiligten Einflussgrößen (5 Ms) beschrieben.

Die darauf folgende **Funktionsanalyse** ordnet jedem Teilsystem und Systemelement bzw. Teilprozess, Prozessschritt und Einflussgröße mindestens eine Funktion bzw. ein Merkmal (als Voraussetzung zur Funktionserfüllung) zu. Die Funktionen werden in einem Funktionsbaum nach den einzelnen Funktionsbeiträgen der Systemelemente verknüpft, so dass ein Funktionsnetz mit logischen Ursache/Wirkung-Beziehungen entsteht.

Die Funktionsanalyse bildet die Grundlage für die anschließende **Fehleranalyse**. Hier werden den einzelnen Funktionen Fehlfunktionen zugeordnet. Bei Verknüpfung der Fehlfunktionen zum Fehlernetz wird ein zentraler Fehler als Basis ausgewählt, welcher mit seinem zugehörigen Systemelement den Fokus der Analyse und damit die Untersuchungstiefe bestimmt. Diesem Fehler werden auf der rechten Seite seine Ursachen, auf der linken Seite seine potenziellen Folgen angehängt.

Die nächsten Schritte bearbeitet man mit Hilfe des FMEA-Formblatts VDA 96 [164], **Bild 4-4**. Nach Übertragung des Fehlernetzes in das Formblatt werden die Auswirkungen des Fehlers und der augenblickliche Ist-Zustand hinsichtlich Vermeidungs- und Entdeckungsmöglichkeiten in der **Risikobewertung** diskutiert und bewertet. Das Risiko eines Fehlers wird durch Bewertung der drei Kennzahlen Bedeutung (B), Auftretenswahrscheinlichkeit (A), Entdeckenswahrscheinlichkeit (E) jeweils von eins (gut) bis zehn (schlecht) und Berechnung der Risikoprioritätszahl (RPZ) aus diesen Kennzahlen durch Multiplikation bestimmt. Die Bewertung der Kriterien A, B und E geschieht anhand eines vorher diskutierten Bewertungskataloges, der durch markante Beispiele während der FMEA dynamisch erweitert werden sollte. Für die vorliegende Arbeit wurde in mehreren FMEA elektronischer Systeme bei mobilen Arbeitsmaschinen ein geeigneter Bewertungskatalog entwickelt (siehe Anhang Kapitel 9.1).

LTM	Fehlermöglichkeits- und -einflussanalyse ☐ System-FMEA Produkt ☐ System-FMEA Prozess								FMEA-Nr.: Seite von
Typ/Modell/Fertigung/Charge:				Sach-Nr.: Änderungsstand:	Verantw.: Firma:				Abt.: Datum:
System-Nr./Systemelement: Funktion/Aufgabe:				Sach-Nr.: Änderungsstand:	Verantw.: Firma:				Abt.: Datum:
Mögliche Fehlerfolgen	B	Möglicher Fehler	Mögliche Fehlerursachen	Vermeidungs-maßnahmen	A	Entdeckungs-maßnahmen	E	RPZ	V/T

Bild 4-4: *Tabellenkopf des FMEA-Formblatts VDA 96 [164].*

Liegt nach abgeschlossener Bewertung die RPZ in einem hohen Bereich, muss das FMEA-Team entscheiden, ob der Anfangsstand im letzten Schritt der FMEA, der **Maßnahmenoptimierung**, verbessert werden muss. So können z. B. erweiterte Vermeidungsmaßnahmen das Auftreten des Fehlers vermindern bzw. neue Entdeckungsmaßnahmen die Möglichkeiten der Fehlerbeherrschung verbessern.

Die Anwendung der Methode System-FMEA ist ein zentraler Punkt im sicherheitsgerichteten Entwicklungsprozess, um potenzielle Systemfehler möglichst frühzeitig zu beseitigen. Schwierigkeiten ergeben sich bei der Berücksichtigung von Einflüssen bei Mehrfachfehlern, da eine logische Fehlerverknüpfung in der Methodik nicht vorgesehen ist. Eine weit verbreitete Methode, die sich u. a. der logischen Verknüpfung von Fehlerursachen widmet, ist die in [168] beschriebene Fehlerbaumanalyse, die für derartige Fälle vorgeschlagen wird.

4.2.1.4 Methoden zu Spezifikation und Design von Software

Lastenheft, Anforderungsanalyse und Pflichtenheft

Im Spezifikationsstadium des Entwicklungsprozesses konkretisieren die Methoden Lastenheft, Anforderungsanalyse und Pflichtenheft die notwendigen Systemeigenschaften. Ihre Vorgehensweise unterscheidet sich dabei nicht bei der Anwendung auf Softwareprojekte oder konventionelle Produkte. Nach DIN 69905 [169] beschreibt das Lastenheft ergebnisorientiert die Gesamtheit der Forderungen an die Lieferungen und Leistungen eines Auftragnehmers. Für die Entwicklung eingebetteter Software von E/E/PE-Systemen, wie sie hier behandelt werden, dokumentiert das Lastenheft die grundlegenden Spezifikationen der zu entwickelnden Software hinsichtlich folgender Anforderungsgruppen:

- **Funktionsanforderungen** (Funktionalität, Überwachungsfunktionen, Diagnosemöglichkeiten, Ausfallstrategien, etc.)
- **Entwicklungsanforderungen** (Zuständigkeiten im Entwicklungsprozess und während des Lebenszyklus der Software, Dokumentationsumfang, verwendete Werkzeuge und Methoden, Testmöglichkeiten, etc.)
- **Integrationsanforderungen** (vorhandene Schnittstellen, verwendete Hardware, Kommunikationssysteme, Peripherie des Steuerrechners, etc.)
- **Qualitäts- und Sicherheitsanforderungen** (zu erfüllende gesetzliche Vorschriften und Regelwerke, Qualitäts- und Sicherheitsstandards, erforderliche Systemintegrität, Zuverlässigkeit und Verfügbarkeit, Dokumentation, etc.)
- **Applikationsanforderungen** (erwartete Umgebungsbedingungen, Störeinflüsse von außen, geforderte Robustheit, etc.)

Mit Hilfe der Anforderungsanalyse werden die Anforderungen des Lastenhefts in erforderliche Tätigkeiten eines strukturierten Projektplans umgesetzt. Als Ergebnis entsteht das so genannte Pflichtenheft. Nach DIN 69905 [169] sind darin die vom Auftragnehmer erarbeiteten Realisierungsvorgaben niedergelegt. Sie beschreiben damit die Umsetzung des vom Auftraggeber vorgegebenen Lastenhefts. In der Praxis verschmelzen oftmals Lastenheft und Pflichtenheft zu einer zusammenfassenden Dokumentation der Anforderungen.

Strukturierte Analyse SA

Bei der Anwendungsentwicklung innerhalb von elektronischen Informationssystemen spielen strukturierte Methoden eine wichtige Rolle und sind für jeden komplexen Softwareentwicklungsprozess unverzichtbar. Die wichtigsten Eigenschaften strukturierter Methoden sind:

- Strukturierte, logische und theoretische Vorgehensweise mit Partitionierung einer umfangreichen Problemstellung auf überschaubare Arbeitsvorgänge.

- Analyse und Dokumentation des gesamten Systems, mit Berücksichtigung der Umgebung und aller Teilsysteme.
- Zerlegung von Funktionen und Systemdaten in handliche Einheiten.
- Strukturiertes Vorgehen nach Checklisten.
- Grundsätzlich einfaches, intuitives und pragmatisches Vorgehen.

Eine Standardlösung, welche die Grundlage für viele strukturierte Methoden bildet, ist die **Strukturierte Analyse** [170], ein datenflussorientierter Ansatz zur graphischen Beschreibung der Aufgabenebene eines Informationssystems. **Bild 4-5** zeigt ein Datenflussdiagramm innerhalb der Strukturierten Analyse für ein allgemeines Informationssystem. Im Diagramm wird der Informationsfluss zwischen den einzelnen Systemelementen und Schnittstellen der Systemgrenzen dargestellt.

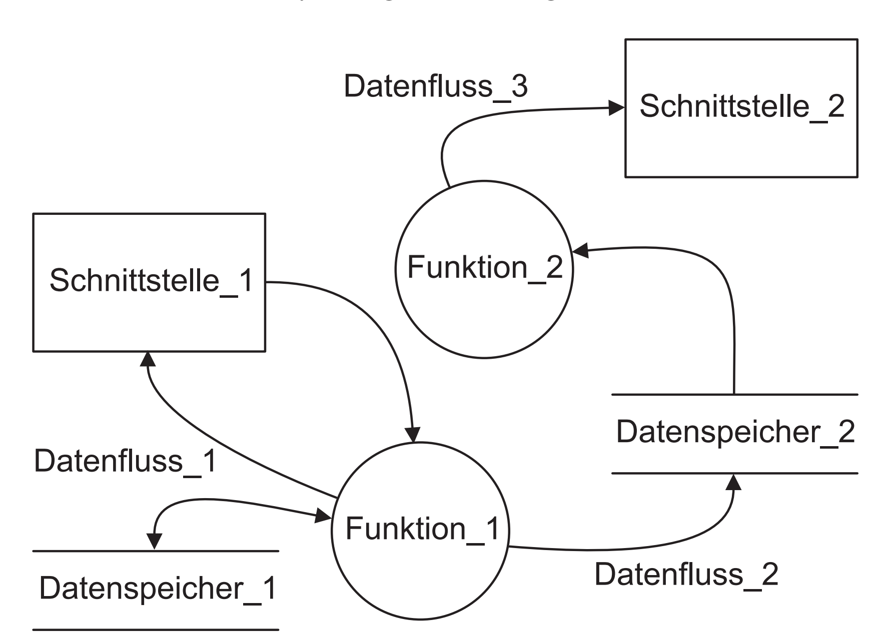


Bild 4-5: *Datenflussdiagramm der Strukturierten Analyse für ein allgemeines Informationssystem mit spezieller Symbolik für die charakteristischen Systemelemente Funktion, Datenfluss, Datenspeicher und Schnittstelle.*

Die Datenflüsse beinhalten die Voraussetzungen für Funktionen oder deren Ergebnisse und werden von Datenspeichern, Systemschnittstellen oder anderen Funktionen bereitgestellt. Die Strukturierte Analyse fasst alle nicht mehr unterteilbaren Datenflussdiagramme in einem Hierarchiemodell zusammen. Weitere Bestandteile sind das Data-Dictionary und die so genannten Mini-Spezifikationen: Im Data-Dictionary werden die Inhalte der Datenflussdiagramme niedergeschrieben, hier bieten sich die Haupteinsatzmöglichkeiten für computergestützte Vorgehensweisen. Mini-Spezifikationen beschreiben das Verhalten von nicht weiter zu detaillierenden Funktionen mit Hilfe von Pseudocode, Entscheidungstabellen oder Entscheidungsbäumen.

Software-Criticality-Analysis SCA

Die Software-Criticality-Analysis ist ein an die Entwicklung von Software angepasstes Verfahren zur Lokalisierung und Analyse sicherheitsrelevanter Softwaremodule [171,

172]. Das Vorgehen ist ähnlich zur vorher beschriebenen FMEA, wobei die zur Realisierung sicherheitsrelevanter Funktionen nötigen Softwaremodule ermittelt und die Auswirkungen möglicher Fehler in diesen Programmteilen aufgezeigt werden. Die Software-Criticality-Analysis identifiziert damit sicherheitsrelevante Softwareteile und bestimmt den nötigen Test- und Überwachungsaufwand abhängig vom Risikopotenzial.

Programmierung nach Softwarestandards

Im Fahrzeugbereich hat sich die nach ISO/IEC 9899 [173] genormte Programmiersprache C am meisten verbreitet. Daneben helfen auf dieser Norm aufbauende Softwarestandards bei der sicherheitsgerechten Umsetzung der Funktionen in Steuergeräte-Code. Ein Beispiel für Programmierrichtlinien für sicherheitskritische Anwendungen in C wurde von der Motor Industry Software Reliability Association (MISRA) entwickelt: Bei MISRA C handelt es sich um derzeitig 127 Programmierregeln, die potenzielle Fehlerquellen bei der Programmierung beseitigen sollen. So werden fehleranfällige Konstrukte verboten, die nach C-Spezifikation standardmäßig zulässig sind. Des Weiteren werden den Standard ergänzende Ratschläge gegeben. Weitere Einzelheiten siehe auch [174, 175].

Konfigurationsmanagement

Die Einflussgrößen strukturierter Softwareentwicklung werden durch Projektmanagement, Systemarchitektur, Qualitätsmanagement und nicht zuletzt durch das Konfigurationsmanagement abgedeckt. Wesentlich ist, dass beim Konfigurationsmanagement das verwendete Werkzeug nicht zur eigentlichen Erstellung der Software, sondern zur Steuerung und Automatisierung von Entwicklungs- und Produktionsabläufen der Software sowie zur Dokumentation der Arbeitsfortschritte und Ergebnisse dient [176]. Konkret wird der gesamte Evolutionsprozess während des Softwarelebenszyklus mit den Aufgaben Versionsverwaltung, Archivierung, Änderungsverfolgung von Entwicklungsständen bis zum kontrollierten Software-Update im realen Fahrzeug [177] begleitet. Komplexe Softwareprojekte bleiben nur mit Hilfe eines durchgängigen Konfigurationsmanagements überschaubar. Die Beachtung von Programmiergrundsätzen, wie Wiederverwendung bewährter Softwaremodule oder Dokumentation bezüglich Reproduzierbarkeit, wird dadurch erleichtert.

4.2.2 Methoden für Test und Validierung

Bei der Beschreibung konventioneller Testmethoden ist es sinnvoll, nach Methoden für komplette mechatronische Systeme und reinen Softwaretestmethoden zu unterscheiden. Die in den mechatronischen Systemen enthaltenen Softwareteile werden in Systemtests als Black-Box betrachtet und innerhalb Funktionalität und Fehlerverhalten des kompletten

Systems mitgetestet. Andererseits konzentriert man sich in reinen Softwaretests auf die Erfüllung der Spezifikationsanforderungen der Software als Systemkomponente.

4.2.2.1 Test von Funktionalität und Fehlerverhalten mechatronischer Systeme

Die Funktionalität sowie das Fehlerverhalten von mechatronischen Systemen kann nach mehreren Kriterien in unterschiedlich konfigurierten Versuchen getestet werden. **Tabelle 4-3** zeigt einen morphologischen Kasten für die Konfiguration und Auswahl von Versuchen hinsichtlich unterschiedlicher Entscheidungskriterien.

Tabelle 4-3: *Morphologischer Kasten zur Bestimmung von Versuchskriterien bei konventionellen Tests mechatronischer Systeme.*

Kriterien	**Varianten**					
Betriebsanforderung	Test der Funktionalität			Test des Fehlerverhaltens		
Systemumfang	Komponente		Teilsystem		Gesamtsystem	
Funktionsauslastung	leicht		schwer		extrem	
Umgebungsbedingungen	standard		erschwert		extrem	
Umgebungsstörfaktoren[a]	Temperatur	Staub	Vibration	Stoß	Feuchte	EMV
Prüfungsumfeld	Prüfstand			realer Einsatz		

a) Prüfverfahren genormt u. a. in ISO 14982 [154], ISO/CD 15003 [156] und ISO 16750 [157]

Beispiel für eine mögliche Extremkonfiguration wären Worst-Case-Szenarios, die gezielt die ungünstigsten Varianten hinsichtlich Funktionsumfang und Umgebungsbedingungen in Verbindung mit mehreren Störfaktoren als Testbedingungen auswählen.

4.2.2.2 Methoden zu Test und Validierung von Software

Die konventionelle Vorgehensweise für Test und Validierung von Software teilt sich in statische Analysen und dynamische Tests. Grundsätzlich unterscheiden sich die beiden Methodengruppen nach den zu behandelnden Testobjekten: Statische Analysen überprüfen Spezifikationsdokumente oder Anforderungsdefinitionen von Softwareprojekten anhand der geforderten Eigenschaften. Dynamische Tests dagegen untersuchen das Verhalten ausführbarer Software(-Teile) auf die korrekte Funktionalität oder das Fehlerverhalten anhand des laufenden Codes. In **Tabelle 4-4** sind die statische und dynamische Analyse gegenübergestellt. In der Praxis wird meistens versucht, die positiven Eigenschaften beider Arten in einer Kombination zu verbinden. Die Vorteile der Methoden zur statischen Analyse liegen dabei in einer möglichen frühen Anwendung während des Soft-

wareentwicklungsprozesses, was das Risiko von aufwendigen Änderungen zu späteren Zeitpunkten verringert. Im Gegensatz dazu können dynamische Tests zusätzlich zu systematischen auch statistische Fehler (zufälliges Versagen einzelner Komponenten, z. B. EMV, Bit-Kipper, etc.) des programmierten Systems erkennen. Die Testabdeckung ist weitreichender und damit näher am Serienprodukt.

Tabelle 4-4: *Unterscheidung von statischen und dynamischen Analyseverfahren bei der konventionellen Softwareentwicklung.*

Statische Analysen	Dynamische Tests
Objekte: • Dokumente (Sourcecode, Protokolle, Berichte, Datenflussdiagramme) • Anforderungsdefinitionen (Lastenheft, Pflichtenheft, Spezifikation, Data-Dictionary)	**Objekte:** • Ausführbarer, kompilierter Code • Programmablauf auf Systemebene • Programmablauf auf Modulebene
Methoden: • Reviews (regelmäßige Überprüfung von Softwareständen) • Erzeugung von Metriken (Quantifizierung der Komplexität, Analyse der Code- bzw. Testabdeckung, Code-Instrumentierung) • manuelle Prüfmethoden, Inspektionen • Syntaxprüfung nach Spezifikation, Programmierregeln, Herstellerstandards	**Methoden:** • Funktionstests (Black-Box-Test) • Test der Fehlerbeherrschung/Überwachungen durch injizierte Fehler • Test der Schnittstellenverarbeitung • Test bezüglich zeitlicher Anforderungen • EEPROM-Simulation • Steuergerätetest im Brettaufbau, Performancetests, Stresstests
Intention: Aufdecken systematischer Fehler	**Intention:** Aufdecken systematischer **und** statistischer Fehler
Nachweis von Funktionalität, Pflegbarkeit, Komplexität und Einhaltung von Softwarestandards	

Viele Entwicklungswerkzeuge, wie die gängigsten Compiler, verwenden integrierte statische und dynamische Testmethoden, um in ihrem Debug-Modus (Fehlererkennung durch Syntaxprüfung am Quelltext, schrittweiser Funktionstest des kompilierten Codes, usw.) möglichst viele Fehler zu erkennen.

Die im nächsten Teilkapitel angesprochenen modellbasierten Methoden zur Softwareentwicklung versuchen die genannten Vorteile beider Testmethoden zu verbinden, fokussieren dabei aber die dynamische Analyse. Eine durchgängige, modellbasierte Vorgehensweise ermöglicht es damit, schon in der frühen Entwicklungsphase Teilfunktionen nach Spezifikation dynamisch testen zu können.

4.3 Modellbasierte Methoden für die Softwareentwicklung

Bei der Entwicklung mechatronischer Systeme unterscheidet man zwei verschiedene Sachverhalte für den Begriff „modellbasiert", einmal die modellbasierte bzw. -gestützte

Regelungstechnik[1)] und die in diesem Kapitel behandelten modellbasierten Entwicklungsmethoden. Modellbasierte Methoden fokussieren Spezifikation und Design von Softwaremodulen mit Einbeziehung der programmierbaren Hardwaresysteme bei den Testmethoden. In partiellen Bereichen des Softwareentwicklungsprozesses wurden in den letzten Jahren immer häufiger konventionelle Methoden durch modellbasierte ersetzt: Unterschiedliche Teilsysteme des mechatronischen Gesamtsystems werden durch Abbildung der Physik und/oder Logik, meist mit Hilfe einer graphisch strukturierten Darstellungsweise, modelliert und in die Entwicklungskette integriert. Die durchgängig modellbasierte Entwicklung von softwarelastigen Systemen ist dagegen noch eine Ausnahme. Grundsätzlich gibt es vier verschiedene Vorgehensweisen bzw. Einsatzbereiche für modellbasierte Methoden während eines Entwicklungsprozesses, die im Idealfall ineinander greifen:

1. Die **Abbildung** des gesamten Systems, einzelner Teilsysteme oder einer Komponente **rein virtuell am Rechner** in der frühen Phase der Funktionsentwicklung, Spezifikation oder Grobauslegung. Beispiele sind modellbasierte Spezifikation, Model-in-the-Loop (MIL) und Software-in-the-Loop (SIL).
2. Einbindung einzelner **Teilsysteme oder Komponenten als reale Hardware** in das simulierte Restsystem im so genannten Hardware-in-the-Loop-Test (HIL).
3. **Modellierung des Reglers** mit Simulationswerkzeugen für den realen Einsatz im Fahrzeug über eine Rapid-Control-Prototyping-Umgebung (RCP). Die Reglerfunktionen und -parameter können über eine **Echtzeithardware mit Benutzerschnittstelle** an der realen Strecke getestet und angepasst werden.
4. Die Verwendung eines **automatischen Code-Generators**, welche erst die durchgängige Entwicklung der Steuergeräteprogrammierung durch die Umsetzung der Reglermodellierung in Serien-Code ermöglicht.

Punkt eins und zwei der Aufzählung verzweigen sich in unterschiedliche Methoden (MIL, SIL oder HIL mit differierenden Systemgrenzen). **Bild 4-6** versucht diese oft verwendeten Begriffe von einander abzugrenzen und erklärt die gebräuchlichen Varianten davon. Beim Hardware-in-the-Loop-Test (oberer Bildteil) wird in allen Varianten hexadezimaler Code (*.*hex*), d. h. kompilierter Serien-Code, auf dem Zielprozessor in einer Simulationsumgebung getestet. Die Schnittstellendefinition Simulation/Realität der HIL-Umgebung erstreckt sich vom simulationslastigsten Fall, dem Processor-in-the-Loop-Test bis zum hardwarelastigsten Fall, der Einbindung des kompletten Maschinensystems über Prüfstandsversuche (HIL-Systemtest). Beispielhaft sind drei verschiedene Schnittstellen zwischen virtueller Simulation und realem System im Bild eingezeichnet.

1) Bei modellbasierter Regelungstechnik werden mit Hilfe von physikalischer Modellierung von Teilsystemen so genannte Zustandsbeobachter entwickelt, die das Verhalten eines Teilsystems plausibilisieren oder sogar vorausschauend beurteilen können, siehe auch Kapitel 6.3.1.

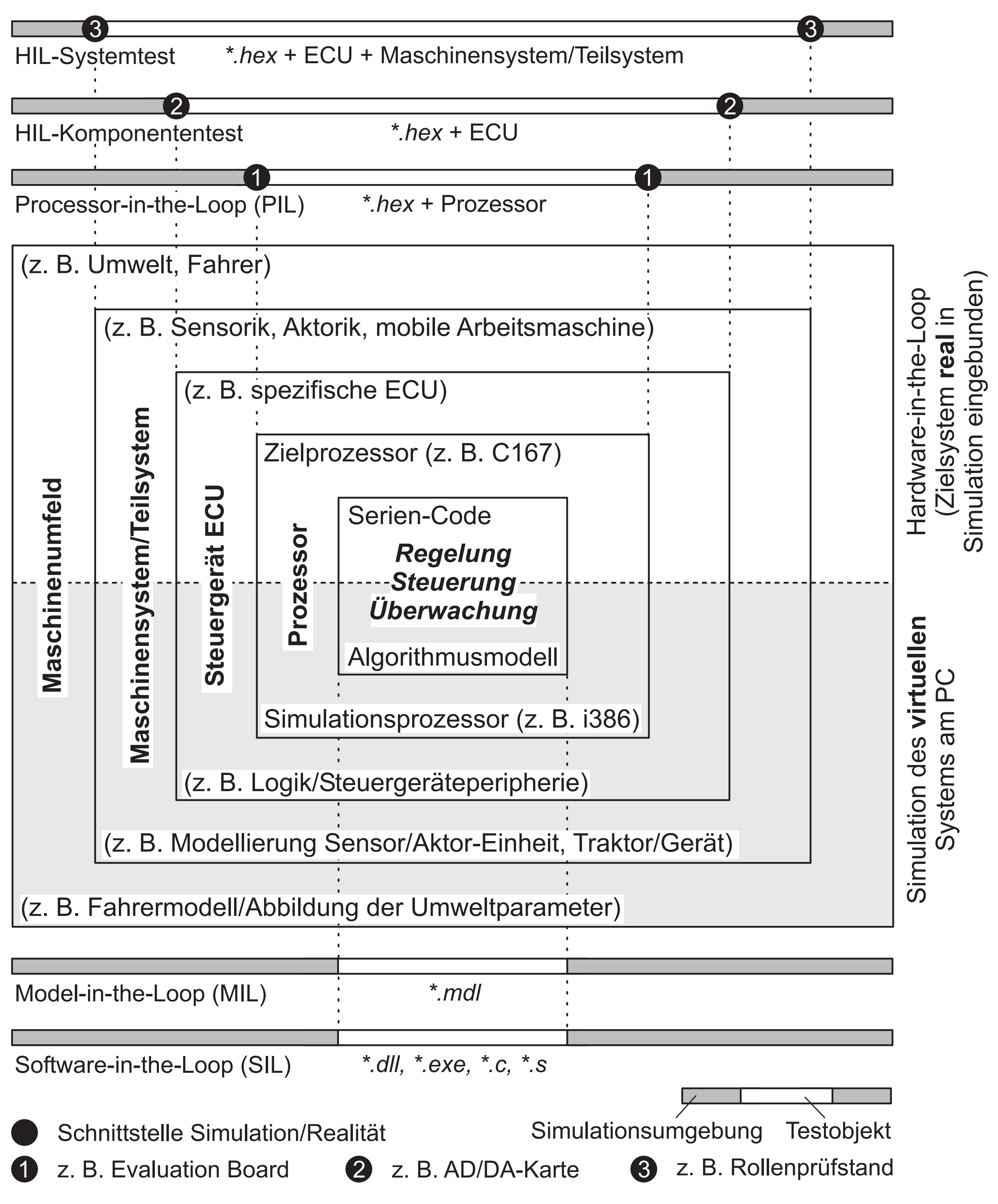


Bild 4-6: *Abgrenzung unterschiedlicher Methoden für die modellbasierte Entwicklung von Serien-Code elektronischer Steuerungen. Dargestellt sind zwei grundsätzliche Ansätze mit ihren Varianten: Einbindung des zu entwickelten Systems in eine Simulationsumgebung (oben) und virtuelle Logikentwicklung am Rechner (hellgrau, unten).*

Der rein virtuelle Test der Logik, siehe unterer Bildteil, testet dagegen Funktionsmodelle (*.*mdl*) im Model-in-the-Loop-Test, bzw. ausführbaren, kompilierten, eingebundenen Code (*.*dll* oder *.*exe*) oder direkt eingebundene Quellcode-Dateien (*.*c* oder *.*s*) im

Software-in-the-Loop-Test. Beide Methoden MIL und SIL testen den Code auf einem von der Zielhardware abweichenden Simulationsprozessor, meist ein PC-basiertes System mit spezieller Simulationssoftware, z. B. Matlab/Simulink [178].

Schon der partielle Einsatz modellbasierter Methoden während der Softwareentwicklung bringt Vorteile, wie Erhöhung der Anschaulichkeit und Transparenz der Systeme, die integrierten funktionellen Testmöglichkeiten und damit kürzere Entwicklungszyklen in Technologiephase, Vorentwicklung und früher Serienentwicklung, mit sich. Der feststellbare Trend, modellbasierte Methoden während des gesamten Entwicklungsprozesses einzusetzen, um damit eine durchgängige Vorgehensweise zu erreichen, erzielt weitere direkt damit verbundene Vorteile:

- Kontinuierliche Bearbeitung der Logik in einem Modell ohne Parallelansätze, z. B. bedingt durch Modellierung und anschließende manuelle Programmierung und damit Vermeidung von Inkonsistenzen, Brüchen und doppelt geleisteter Arbeit.
- Die Umsetzung der Funktionen (Modellierung) ist unabhängig von der Testmethode zu jedem Zeitpunkt der Entwicklung.
- Erleichterung von Dokumentation und Konfigurationsmanagement durch Verwendung von Modellbibliotheken während des gesamten Entwicklungsvorgangs vom Lastenheft bis zum fertigen wieder verwendbaren Softwaremodul.

Bild 4-7 zeigt unterschiedliche Einsatzzeitpunkte modellbasierter Methoden bei der Entwicklung mechatronischer Systeme. Eine durchgängige Einführung zieht einen umfassen-

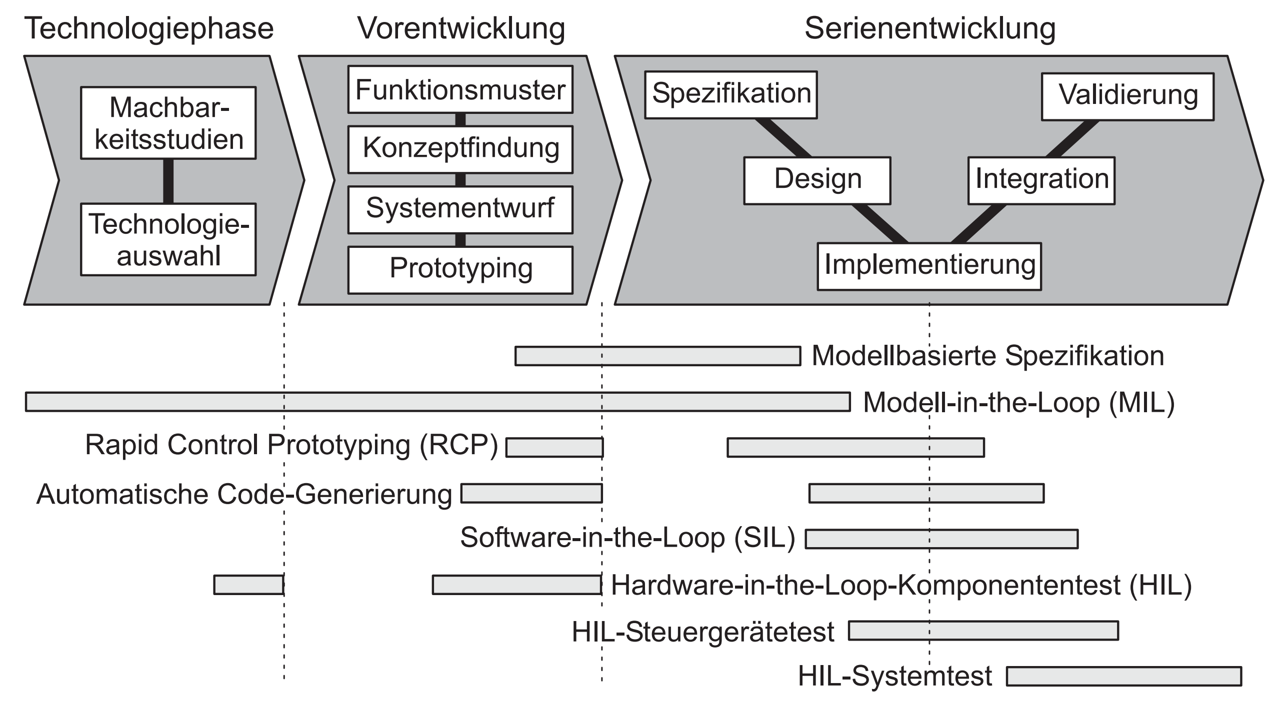


Bild 4-7: *Anwendungsphasen modellbasierter Methoden im Entwicklungsprozess für mechatronische Systeme.*

den Veränderungsprozess nach sich, den es zu managen gilt. In [179] werden Szenarios und Schritte für die Einführung vorgeschlagen, die auf die Entwicklungsvorgänge bei elektronischen Systemen auch bei mobilen Arbeitsmaschinen angewandt werden können. Die folgenden Beschreibungen modellbasierter Methoden sind in der Reihenfolge aufgeführt, in der sie während eines durchgängig modellbasierten Entwicklungsprozesses angewandt werden könnten.

4.3.1 Modellbasierte Spezifikation

Die modellbasierte Spezifikation ist eine Erweiterung der konventionellen Vorgehensweise mit rechnergestützten, modellbasierten Elementen. Wie im konventionellen Fall liegt ihre Hauptanwendung in der ersten Phase der Serienentwicklung, wobei auch Bereiche der Vorentwicklung davon profitieren können. Schon mit der Konzepterprobung in der Vorentwicklung oder früher Festlegung der Anforderungen in der Serienentwicklung werden Basisfunktionen definiert und mit Hilfe von Simulationswerkzeugen (z. B. Matlab/Simulink/Stateflow [178]) abgebildet. Die modellbasierten Funktionsbeschreibungen sind direkt an die Funktionalität des Teilsystems oder der Komponente gekoppelt und werden in die textbasierte Spezifikation (z. B. mit Hilfe der Softwarelösung DOORS [180]) integriert und verwaltet, siehe auch **Bild 4-8**.

Bei der konsequenten Anwendung von modellbasierter Spezifikation lassen sich Modellbibliotheken aus Spezifikationsdaten einzelner Funktionen aufbauen. Bestandsmerkmale von modellbasierten Lastenheften sind:

- **Textbasierte** Informationen, wie einzuhaltende Richtlinien, qualitative Beschreibungen und Parametrierungen.
- **Modellbasierte** Informationen, wie Zustandsmaschinen, Regelkreise und mathematisch logische Funktionsstrukturen.

Eine durchgängige Werkzeugkette für modellbasierte Spezifikation aus dem textbasierten Spezifikationswerkzeug DOORS, der mathematisch logischen Simulationsumgebung Matlab, Simulink, Stateflow und einer zusätzlichen Softwarelösung für Versions- und Konfigurationsmanagement wird ausführlich in [181] beschrieben. Im weiteren Vorgehen werden die spezifizierten, modellierten Teilfunktionen zu Gesamtfunktionalitäten (Steuerung/Regelung/Überwachung) zusammengefügt und im Model-in-the-Loop-Test weiter entwickelt.

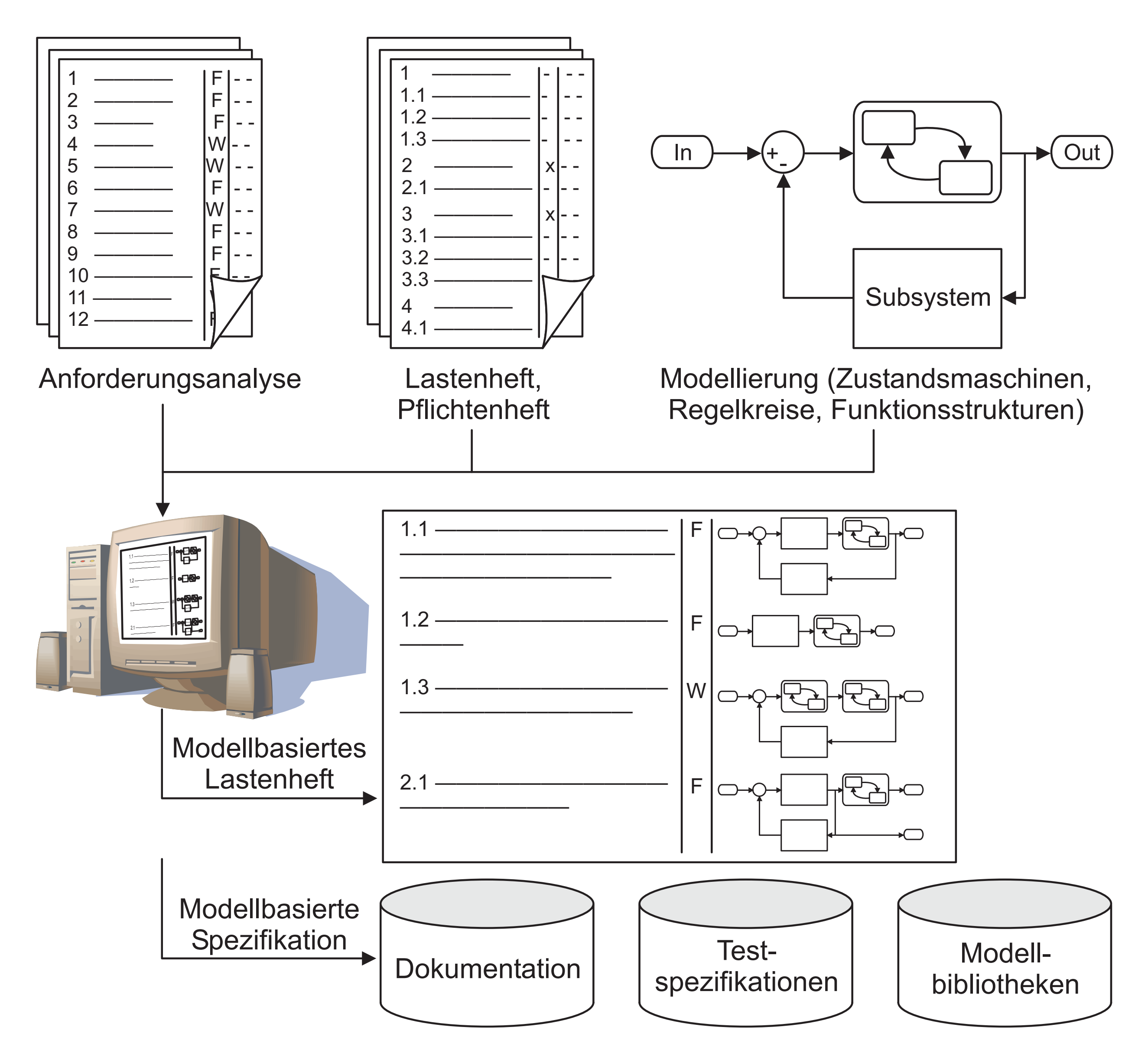


Bild 4-8: *Prinzip der Vorgehensweise modellbasierter Spezifikation am Rechner. Die Erarbeitung eines modellbasierten Lastenhefts am PC bietet die Grundlage systembeschreibender Spezifikationsdatenbanken.*

4.3.2 Model-in-the-Loop (MIL)

Model-in-the-Loop ist die moderne Bezeichnung für klassische simulationsbasierte Funktionsentwicklung. So wird z. B. das simulierte Modell einer zu entwickelnden Logik in die Simulation der Strecke eingebunden und kann am Rechner schon in der frühen Phase der Entwicklung gefahrlos untersucht werden. Das im **Bild 4-9** dargestellte typische mechatronische System einer mobilen Arbeitsmaschine wird demnach komplett virtuell inklusive Umgebungsparameter, Fahrerverhalten und Physik simuliert. Die Detaillierung und Genauigkeit der Abbildung der Strecke richtet sich dabei nach den Anforderungen der zu entwickelnden Algorithmen. Ein Beispiel für eine Simulationsumgebung ist die Werk-

zeugkette Matlab/Simulink/Stateflow [178], die auch im Rahmen dieser Arbeiten verwendet wurde.

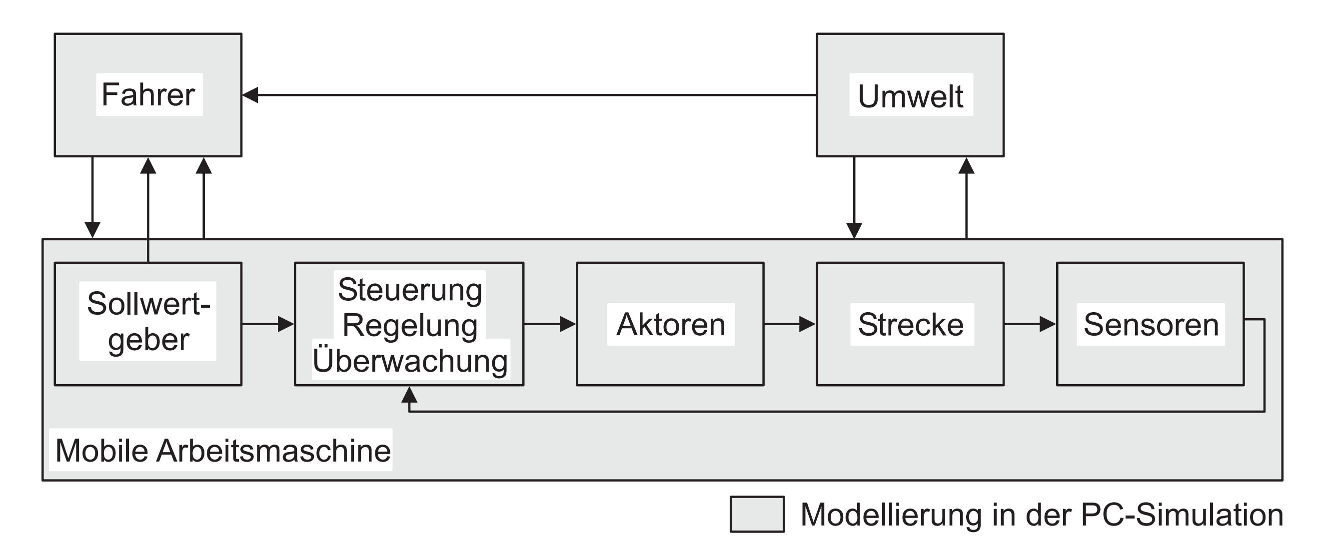


Bild 4-9: *Mathematisch logische Abbildung des mechatronischen Systems im Model-in-the-Loop-Test.*

Das in der Simulation validierte Reglermodell kann im nächsten Schritt der modellbasierten Entwicklung mit Hilfe einer Rapid-Control-Prototyping-Umgebung im Fahrzeug online getestet und optimiert werden.

4.3.3 Rapid-Control-Prototyping (RCP)

Der Ausgangspunkt einer Entwicklung nach dem Prinzip „Rapid-Control-Prototyping“ ist die Abbildung der zu entwickelnden Regler- oder Steuerungsstrukturen in der MIL-Simulation. Die modellierte Logik soll auf einem echtzeitfähigen Entwicklungsrechner im realen Fahrzeugeinsatz weiterentwickelt werden. Das Reglermodell wird dafür, konform der Schnittstellen des realen Seriensteuergerätes, aus der Gesamtsimulation freigeschnitten und mit werkzeugspezifischen Simulationsblöcken für Ein- und Ausgänge erweitert, **Bild 4-10**. Im günstigsten Fall parametrisiert man die Ein- und Ausgabeschnittstellen (I/O) direkt über standardmäßige Simulationsblöcke. Reicht dagegen der Signalbereich nicht aus, muss die Anpassung über eine externe Signalkonditionierung erfolgen. Aus dem angepassten, echtzeitfähigen Modell wird eine lauffähige Anwendung mit geeigneten I/O-Schnittstellen aus der Simulation generiert und auf der Echtzeithardware zur Ausführung gebracht. Für die RCP-Hardware werden Rechnersysteme, meist Power-PC-basierte Hochleistungsprozessoren mit weit höherer Leistungsfähigkeit als das Seriensteuergerät (z. B. die RCP-Hardware MicroAutoBox der Fa. dSPACE [182]) eingesetzt, um Einschränkungen der Zielhardware zu vermeiden. Ein Sonderfall des normalen Rapid-Control-Prototyping (Fullpass) ist die Verwendung eines RCP-Systems als Bypass-Lösung:

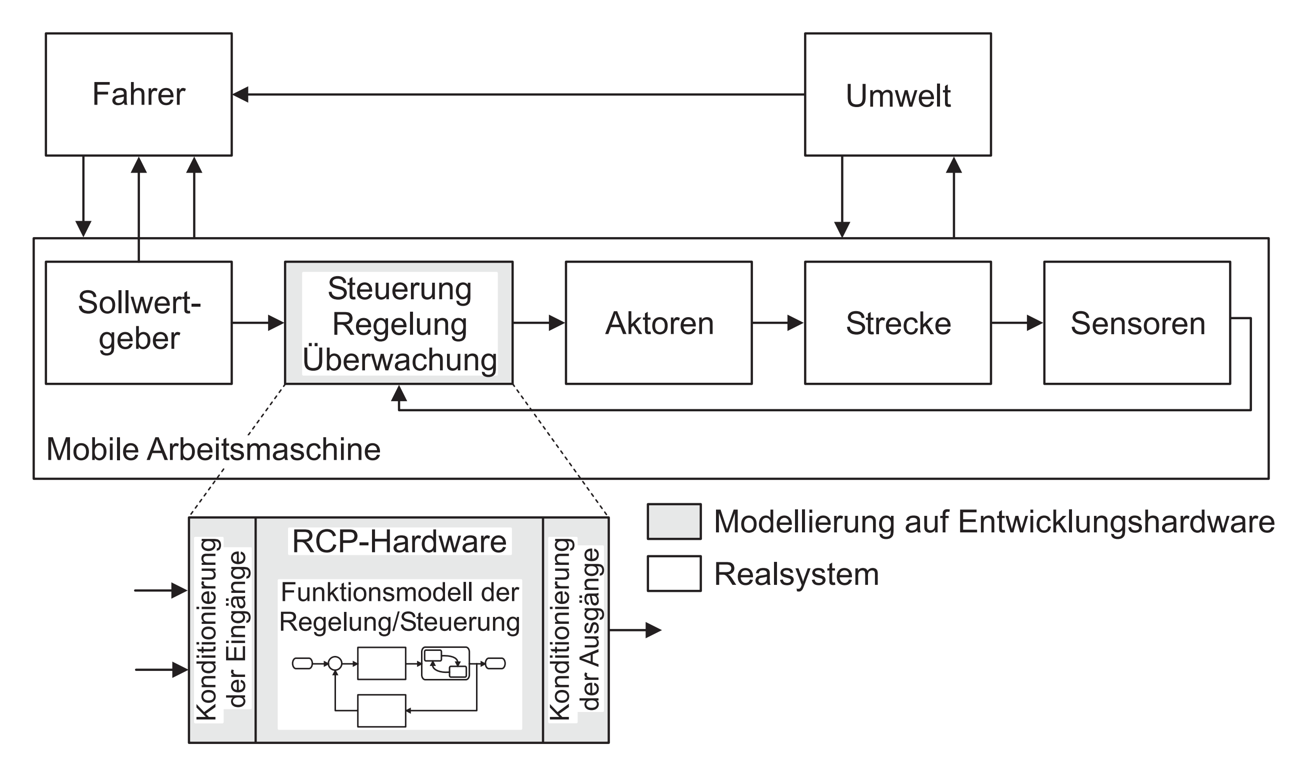


Bild 4-10: *Funktions-Prototyping mit Hilfe eines Fullpass-RCP-Systems. Das Modell der zu entwickelten Algorithmen wird auf einer Echtzeithardware ausgeführt und im realen Fahrzeug online optimiert.*

Einzelne, zu entwickelnde Funktionen werden auf die RCP-Hardware ausgelagert, wobei das Seriensteuergerät in seinem normalen Betrieb (mit Ausnahme der ausgelagerten Funktionen) weiter arbeitet. Die beiden Rechner werden über eine Echtzeitschnittstelle synchronisiert und der Datenaustausch gewährleistet, siehe auch [183]. Die Vorteile einer RCP-Entwicklungsumgebung liegen in der einfachen, intuitiven Modifizierung der Algorithmen in der Modellierung und der Möglichkeit, online Parameter, Variablen oder Zustände zu diagnostizieren und in Echtzeit im realen Fahrzeug zu verändern.

4.3.4 Software-in-the-Loop (SIL)

Eine Möglichkeit, den konventionell programmierten Steuergeräte-Code in der Simulation zu testen, ist der Software-in-the-Loop-Test. Einzelne programmierte Funktionen oder umfassendere Funktionsstrukturen lassen sich über spezielle Simulationsblöcke in das Gesamtmodell in Form von ausführbaren Code-Dateien (**.dll, *.exe*) oder als Quellcode (**.c, *.m, *.s*) einbinden. Sie übernehmen die Funktionalität des Reglers, der Steuerung oder der Überwachung – das Restsystem bleibt wie beim MIL-Test komplett simuliert. Bei Einbettung der Code-Module müssen die Schnittstellen zur Simulation hinsichtlich Typisierung und Wertebereich der übergebenen Variablen in den speziellen Simulationsblöcken konfiguriert werden. In **Bild 4-11** ist ein Beispiel für den Funktionstest mittels Software-in-the-Loop gezeigt.

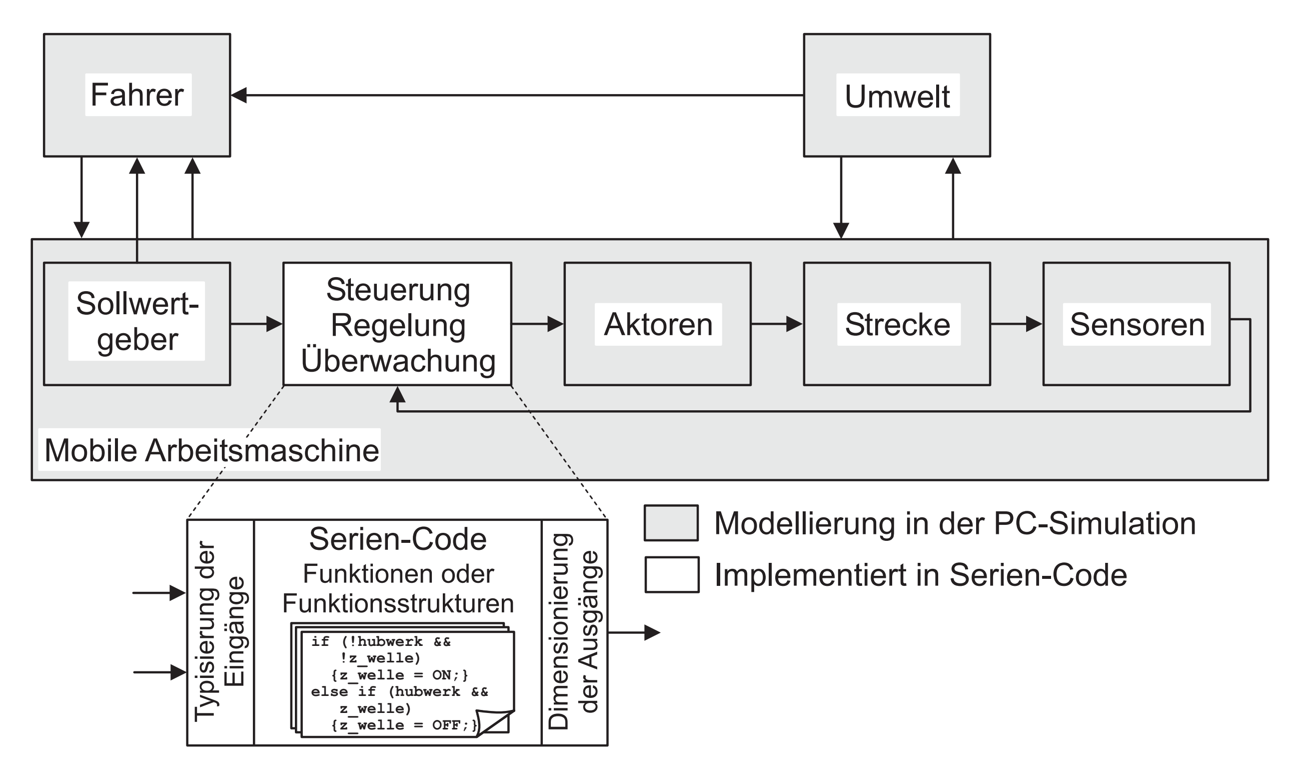


Bild 4-11: *Beispiel einer Software-in-the-Loop-Simulation mit Einbindung des programmierten Serien-Codes in die Gesamtsimulation am Rechner.*

Der Test kompletter Steuergeräteprojekte mit der SIL-Methode ist allerdings sehr aufwendig, da steuergerätespezifische Funktionen, Task-Steuerung und Unterschiede bezüglich Ganzzahl- und Fließkommaarithmetik extra berücksichtigt werden müssen.

4.3.5 Automatische Generierung von Serien-Code

Auch wenn die modellierten Funktionen im frühen Entwicklungsstadium ausgiebig getestet werden konnten (MIL), fehlt bei der späteren konventionell manuellen Codierung die direkte Weiterverwendbarkeit der erstellten Logiken. Die erstellten Blockschaltbilder oder Zustandsmaschinen dienen zwar als graphische Spezifikation, müssen aber von Hand in endgültigen Code für die Produktion in der Serie umgesetzt werden. Das bedeutet einen Bruch und zweigleisiges Vorgehen bei der weiterführenden Entwicklungsarbeit hinsichtlich der zwei Linien „Modellstruktur“ und „manuelle Umsetzung in C-Code“. Beispielsweise müssen nach der Codierung gefundene Fehler im entsprechenden Funktionsmodell verbessert und verifiziert, parallel dazu die Implementierung in C-Code entsprechend angepasst werden.

Die Vorteile einer durchgängig modellbasierten Entwicklung von Software lassen sich nur durch eine konsequente Weiterverwendung der entwickelten Funktionsmodelle für die Codierung des Seriensteuergeräts nutzen. Als modernes Hilfsmittel sind automatische Code-Generatoren erhältlich, die auf Basis der modellierten und verifizierten Funktionen

normal lesbaren und kommentierten Serien-Code für den entsprechenden Zielprozessor erzeugen [184, 185]. Nachträgliche Änderungen des Modells können so direkt durch automatische Umsetzung der Funktionen im Serien-Code berücksichtigt werden. Neben der einfacheren Vorgehensweise ergeben sich weitere Vorteile bei Variantenpflege, Versionsverwaltung und Dokumentation der einzelnen Änderungsstände.

Der Standardanwendungsbereich automatischer Code-Generierung ist die Umsetzung einzelner Funktionsmodule und nicht die vollständige Generierung eines kompletten Softwareprojekts für ein Steuergerät. Das Problem dabei ist die Abbildung steuergerätespezifischer Funktionen für Betriebssystem oder Peripherie, die nur schwer mit Hilfe des Generierungswerkzeugs berücksichtigt werden können. Die generierten Funktionen müssen deshalb nachträglich von Hand in das konventionell programmierte Code-Gerüst eingebettet werden. Eine andere Möglichkeit, welche die spezifischen Funktionen eines Steuergeräts mit berücksichtigt, ist die Einbindung dieser Funktionen als Custom-Code-Blöcke (Simulationsblöcke mit konventionell programmierten Benutzer-Code) in die graphische Programmierung schon vor dem Generierungsprozess. Dadurch entsteht ein Simulationsgerüst, welches an das zu bedienende Steuergerät angepasst wurde und als Rahmen für die eigentlichen Funktionsmodelle fungiert. Beim Generierungsprozess wird dann der gesamte Quell-Code für das Steuergerät erzeugt.

Im Rahmen der Forschungsarbeiten wurde der automatische Code-Generator TargetLink der Fa. dSPACE [182] verwendet und ein komplettes Rahmenmodell für die Realisierung von Softwareprojekten einer universell programmierbaren Steuereinheit abgebildet (Typ ESX 2, C167 Mikrocontroller, Fa. Sensor-Technik Wiedemann). Die Funktionen werden dabei in Matlab/Simulink/Stateflow entwickelt, sind Model-in-the-Loop testbar und können direkt aus der Simulation in den fertigen, kompletten Serien-Code für das Steuergerät überführt werden, siehe auch Kapitel 6.3.4.

Gerade bei sicherheitskritischen Anwendungen ist die Zuverlässigkeit von Entwicklungswerkzeugen von hoher Bedeutung. Die automatischen Code-Generatoren betrifft dies genauso, wie Compiler oder Werkzeuge zur Code-Übertragung auf das Steuergerät, die so genannten Flash-Werkzeuge. In Sicherheitsnormen wird deshalb die Verwendung von bewährten bzw. zertifizierten Werkzeugen gefordert. Beim Nachweis der Betriebsbewährtheit der automatischen Code-Generierung ist die Zuverlässigkeit des Generators, des Rahmenmodells und des standardmäßig eingesetzten Compilers unter konventioneller Testtiefe nachzuweisen. Zum Vergleich ergibt sich bei Verwendung eines zertifizierten Werkzeugs eine geringere Testtiefe, aber nur bezüglich des eigentlichen Generierungsprozesses. Die gewohnten Entwicklungstests der übrigen Ebenen bezüglich Funktionalität, Fehlerverhalten und Spezifikation müssen wie gewohnt durchgeführt werden. Damit wird der Vorteil zertifizierter Werkzeuge relativiert.

Eine durchgängige modellbasierte Softwareentwicklung bietet das Potenzial, sowohl die Sicherheit als auch die Zuverlässigkeit von E/E/PE-Systemen zu verbessern. Hauptgrund dafür ist die stetige Weiterentwicklung und Testbarkeit der Funktionsmodule auf einer durchgängigen Plattform von der Spezifikation bis zur Implementierung mit automatischer Umsetzung eins zu eins in Serien-Code.

4.3.6 Hardware-in-the-Loop (HIL)

Der Hardware-in-the-Loop-Test ist eine effektive Methode, die entwickelten Steuerungen, Regelungen oder Überwachungen auf ihre Funktionalität und Zuverlässigkeit zu testen, Grundlagen siehe [186]. Dabei können unterschiedliche Schnittstellenlagen zwischen virtuellem System (Loop) und realem (Teil-)System (Hardware) ausgewählt werden. Im Gegensatz zum virtuellen MIL-Test können die programmierten Algorithmen auf der endgültigen Hardware in Zielkonfiguration getestet werden, indem sie über eine Echtzeitschnittstelle in das simulierte Restsystem eingebunden sind. Die häufigste Anwendung von HIL ist der Test von elektronischen Seriensteuergeräten in einer virtuellen Umgebung, wie es in **Bild 4-12** gezeigt ist. Oftmals kann es von Vorteil sein, zusätzliche Komponenten, Teilsysteme (z. B. Sensoren, Aktoren, Sollwertgeber) oder das komplette System als Hardware real mit in den Test aufzunehmen. Das Spektrum der Hardware-in-the-Loop-Simulation reicht damit vom einzelnen Prozessor, dem so genannten Processor-in-the-

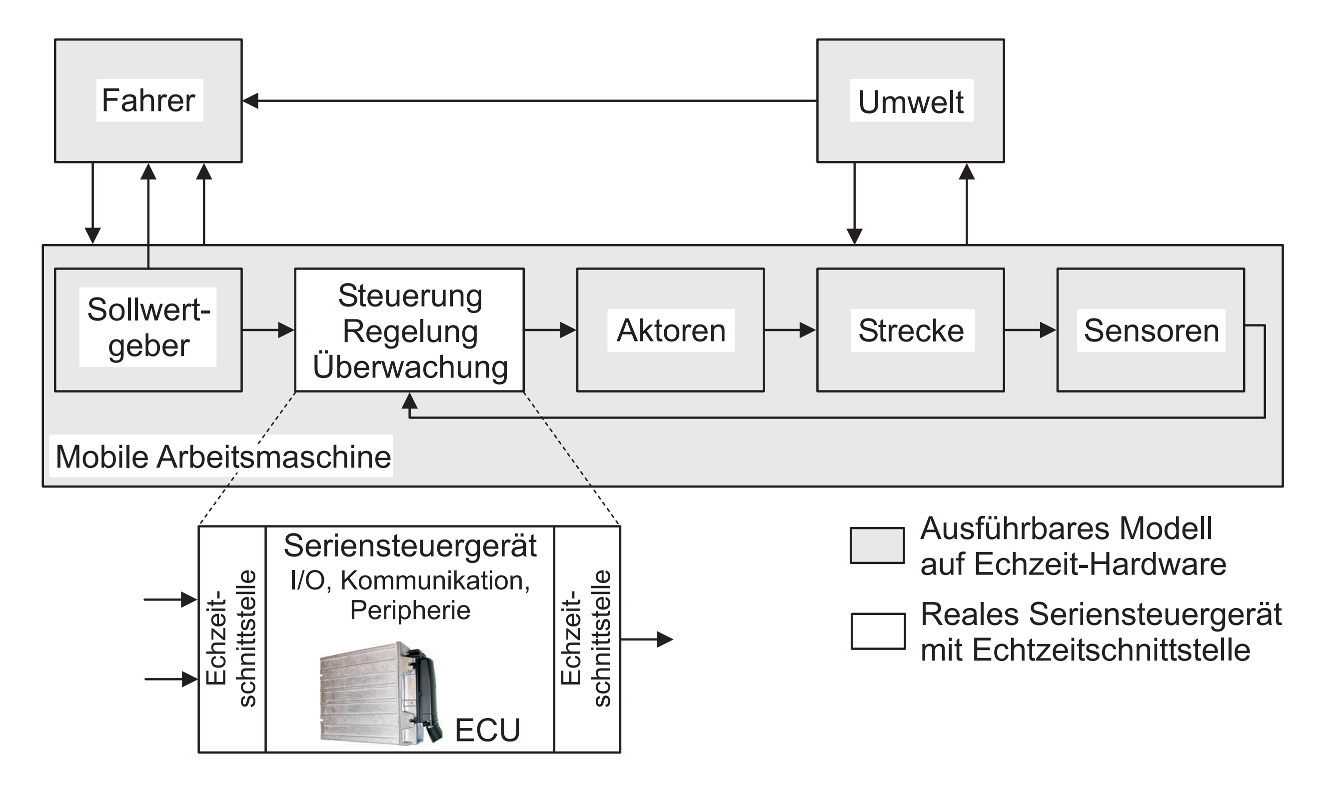


Bild 4-12: *Beispielkonfiguration eines Hardware-in-the-Loop-Tests für ein elektronisches Seriensteuergerät. Die ECU ist über die Echtzeitschnittstelle eines HIL-Prüfstands in die Simulation des Restsystems eingebunden.*

Loop, bis zum kompletten Maschinensystem inklusive Fahrer, welches dann über eine spezielle Prüfstandsanbindung an die Simulation gekoppelt ist. Der obere Teil im vorigen Bild 4-6 zeigt die unterschiedlichen Varianten.

Um das Systemverhalten der Simulation möglichst realistisch abzubilden, ist die Echtzeitfähigkeit des Modells und der Simulationsplattform maßgeblich. Gängige HIL-Prüfstände verwenden Hochleistungsrechner, die exklusiv für die Berechnung des simulierten Systemverhaltens zuständig sind, Beispielsysteme siehe [187, 188]. Die Antwortzeiten des Simulationsrechners liegen in aller Regel weit unterhalb der Taktzeiten des Seriensteuergeräts, womit ein realistisches Zeitverhalten gewährleistet ist. Die Interaktion des Benutzers mit der Simulationsumgebung erfolgt meistens über einen externen Rechner, der die Testbedienung, Diagnose, Datenaufzeichnung, Testautomatisierung oder Einflussnahme auf Systemparameter in Echtzeit erlaubt.

5 Sicherstellung der erforderlichen Systemintegrität – Entwicklungskonzept

Je höher das Gefährdungspotenzial eines Maschinensystems liegt, desto intensiver müssen Mittel der hinweisenden und funktionalen Sicherheit eingesetzt werden, um die für einen sicheren Betrieb notwendige Risikominderung zu erreichen. Das Gefährdungspotenzial eines funktionalen Sicherheitssystems bestimmt direkt seine erforderliche Integrität, d. h. die Fähigkeit, seine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen. Für die Sicherstellung der erforderlichen Integrität eines mechatronischen Systems gibt es grundsätzlich zwei Nachweise bzw. Vorgehensweisen:

- **Nachweis der Systemzuverlässigkeit:** Nachgewiesen wird die sicherheitsgerechte Systemarchitektur unter Verwendung zuverlässiger Komponenten. Die stochastische Zuverlässigkeit der Komponenten und Teilsysteme wird mathematisch logisch verknüpft und zu einer qualitativ vergleichbaren Gesamtzuverlässigkeit zusammengefasst. Nach EN 61508 [151] ist jedem Safety-Integrity-Level eine entsprechende maximale Ausfallwahrscheinlichkeit zugeordnet, die das zu entwickelnde System nicht überschreiten darf (ausführliche Beschreibung der Zuverlässigkeitsanalyse siehe in [153]).
- **Nachweis einer sicherheitsgerechten Systementwicklung:** Nachgewiesen wird das dokumentierte Vorgehen anhand eines sicherheitsgerechten Entwicklungsprozesses mit Vorgehensmodell, Entwicklungsschritten, Methoden und Maßnahmen. Der Entwicklungsprozess ist an die erforderliche Systemintegrität angepasst.

Bei zunehmendem Grad der Elektronifizierung wird es immer schwieriger, die Zuverlässigkeit der Systeme nachzuweisen. Zum einen ist es sehr aufwendig, Ausfallsicherheiten von Software genau zu quantifizieren, zum anderen ist die logische Verknüpfung einzelner Bauteile komplexer, elektronischer Geräte zu einer Gesamtzuverlässigkeit fragwürdig. Gerade die hohe Anzahl von Bauteilen elektronischer Steuergeräte macht eine Aussage über die Gesamtzuverlässigkeit fast unmöglich. Aus diesem Grund wird in vorliegender Arbeit ein Entwicklungskonzept vorgestellt, das auf einer sicherheitsgerechten Syste-

marchitektur aufbaut und an das Risikopotenzial angepasste Entwicklungsprozesse postuliert. Fail-Safe-Architektur, Entwicklungsschritte, Methoden und Maßnahmen werden somit abhängig von der erforderlichen Systemintegrität festgelegt.

Das aktuelle Kapitel stellt einige zum Erreichen der geforderten Systemintegrität möglichen Systemarchitekturen vor und beschreibt das Entwicklungskonzept von der Spezifikation bis zur Validierung. Bestehend aus dem Vorgehensmodell und der Zuordnung von Methoden bzw. Maßnahmen zu den einzelnen Entwicklungsschritten dient es als Vorschlag für eine sicherheitsgerechte Entwicklung von mechatronischen Systemen bei mobilen Arbeitsmaschinen und wurde mit dem Stand der Technik und den aktuellen Sicherheitsnormen abgeglichen.

5.1 Sicherheitsgerechte Systemarchitektur

Innerhalb der zwei Klassen von Fail-Safe-Strategien, Fail-Operational und Fail-Silent (Bild 3-2), gibt es verschiedene Abstufungen von Architekturen für fehlertolerantes bzw. integeres Systemverhalten, siehe auch [189]. Unterschieden wird nach der verfügbaren Zahl redundanter Signalquellen (Kanäle), der zur Auslösung der Sicherheitsfunktion notwendigen Anzahl fehlerhafter Signalquellen und interner Vorkehrungen zur Selbstprüfung. Die Architekturen werden nach EN 61508 [151] mit der jeweiligen Abkürzung „xooy“ (x out of y) klassifiziert, womit man andeutet, wie viele x fehlerhafte der y vorhandenen redundanten Kanäle zur Auslösung der Sicherheitsfunktion herangezogen werden. Sind interne Diagnosemöglichkeiten und Selbstprüfung vorgesehen, erhöht sich die Anzahl der verfügbaren Signalquellen um einen Grad, was mit dem Zusatz „D“ gekennzeichnet wird. Die Symbole für die einzelnen in den Illustrationen verwendeten Systemkomponenten und Operatoren sind in der Legende **Tabelle 5-1** erklärt.

Tabelle 5-1: *Legende der Symbole zu den Darstellungen von Musterarchitekturen für integere und fehlertolerante Systeme.*

Symbol	Bedeutung
SF	Sicherheitsfunktion: Warnmeldung und Abschalten bei Fail-Silent-Systemen. Warnmeldung und Notbetrieb bei Fail-Operational-Systemen.
D	Diagnose, Selbstprüfung
=/≠	Qualitativer Vergleich zweier Signale
Voter	Qualitativer Vergleich und Auswahl aus mehreren Signalen
≥1	Oder-Verknüpfung
&	Und-Verknüpfung
⊶	Unterbrecher, Schalter

Die 1-kanalige Ausführung eines Systems kann nur durch Vorsehen einer Diagnosemöglichkeit durch Selbstprüfung (D) integer ausgelegt werden (Architektur „1oo1D“, **Bild 5-1**). Durch die interne Überwachung wird der sicherheitskritische Fehler erkannt und die Sicherheitsfunktion ausgeführt. Das heißt, das System wird unter Fehlermeldung Fail-Silent abgeschaltet.

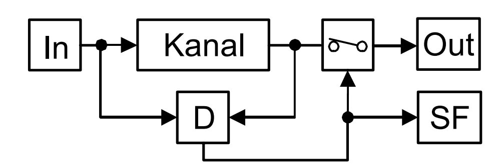


Bild 5-1: *1-kanalige,* ***integere*** *1oo1D-Architektur mit Selbstprüfung. Sicherheitsfunktion: Warnmeldung und Abschalten*

Eine weit verbreitete Variante ist die 2-kanalige Struktur aus **Bild 5-2**, wo durch den Vergleich zweier Kanäle ein potenzieller Fehler festgestellt werden kann. Die nötigen Maßnahmen sind auch in diesem Fall die ausgesprochene Fehlermeldung und das Abschalten des Systems, wodurch eine Weitergabe falscher Systemausgänge vermieden wird. Das 1oo2-System ist somit eine typische Anwendung für gewünschtes Fail-Silent-Verhalten.

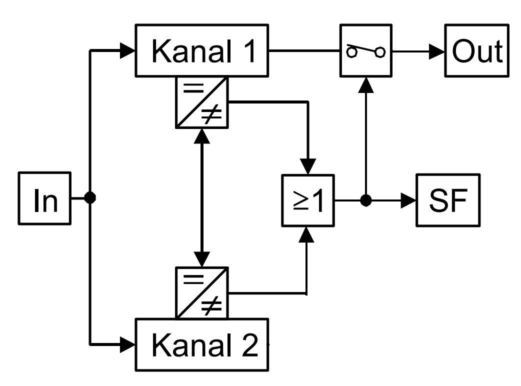


Bild 5-2: *2-kanalige,* ***integere*** *Architektur „1oo2“ mit Vergleich. Sicherheitsfunktion: Warnmeldung und Abschalten*

Bei Systemarchitektur „2oo2“ (**Bild 5-3**) wirkt sich der Vergleich beider Kanäle gegenseitig über Kreuz auf die Gültigkeit des jeweiligen Signals aus. Für ein Auslösen der Sicherheitsfunktion sind in beiden Vergleichern erkannte Fehler die Voraussetzung, wodurch die Verfügbarkeit des Gesamtsystems gesteigert werden kann. Eine festgestellte Abweichung beim Vergleichstest muss aber durch Warnmeldungen angezeigt werden. Wie auch bei den vorigen Systemen führt ein kritischer Fehler zum integeren Ausfall des Systems, da nicht festgestellt werden kann, welcher Kanal fehlerhaft ist. Das System kann dadurch aber fehlersicher abgeschaltet werden.

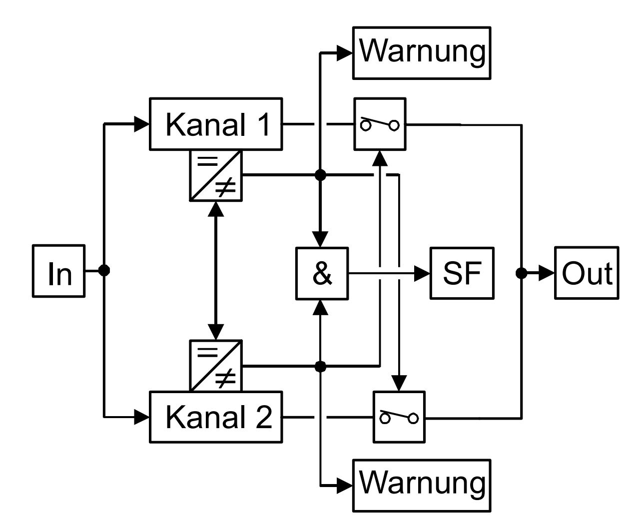


Bild 5-3: *2-kanalige,* ***integere*** *Architektur „2oo2“ mit Kreuzvergleich. Die Sicherheitsfunktionen (Warnmeldung mit Abschalten) werden erst bei Ansprechen beider Vergleicher eingeleitet (hohe Verfügbarkeit des Systems).*

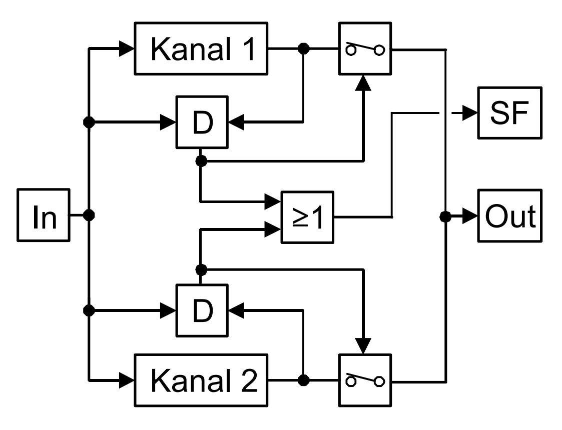


Bild 5-4: *2-kanalige,* ***fehlertolerante*** *Architektur „1oo2D“ mit Selbstprüfung. Sicherheitsfunktion: Warnmeldung, Notbetrieb*

Eine einfach zu realisierende fehlertolerante Struktur (Fail-Operational) ist in **Bild 5-4** gezeigt. Das 2-kanalige System „1oo2D“ ist jeweils mit Einrichtungen zur Selbstprüfung ausgerüstet, wodurch der fehlerhafte Kanal eindeutig bestimmt werden kann. Die Funktionalität des Gesamtsystems bleibt nach dem ersten Fehler sichergestellt (Ein-Fehler-Sicherheit) – Sicherheitsfunktionen, wie z. B. Warnmeldungen und Einleiten des Notbetriebs, werden eingeleitet. Auch in diesem Zustand ist das System zwar nicht mehr fehlertolerant für den Zweitfehler aber immer noch integer. Nach dem zweiten Ausfall muss das System demnach Fail-Silent abgeschaltet werden.

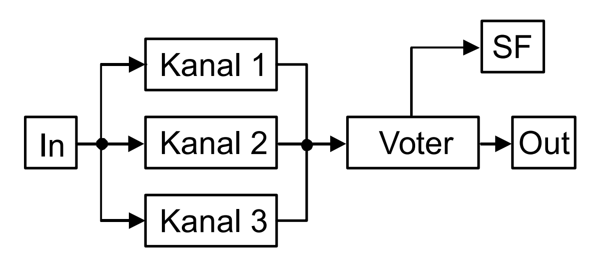


Bild 5-5: *3-kanalige,* ***fehlertolerante*** *Architektur „2oo3“. Sicherheitsfunktion: Warnmeldung und Notbetrieb*

Weit verbreitete fehlertolerante Systeme arbeiten mit Entscheidungslogiken, so genannten Votern, und mehrkanaligen Anordnungen, **Bild 5-5**. Die Eingangsgrößen können dabei durch echte Hardware-Redundanz gemessen oder analytische Redundanz über Prozessmodelle hergeleitet werden. Im dargestellten System mit 2oo3-Entscheidung wird der Einfachfehler funktionssicher beherrscht. Nach einem Zweitfehler bleibt dieses System zwar noch integer, es kann aber nicht festgestellt werden, welcher der übrigen Kanäle fehlerhaft ist, d. h. das System ist dann abzuschalten. Der Ausbau zu höheren Fehlersicherheiten wird durch Hinzufügen weiterer redundanter Kanäle realisiert, z. B. 2oo4-Architektur.

Die erforderliche Systemintegrität bestimmt als Resultat der Risikoanalyse die notwendige Systemarchitektur hinsichtlich ihrer Fehlertoleranz, siehe **Tabelle 5-2**.

5.2 Vorgehensmodell für System- und Softwareentwicklung

Die in Kapitel 4.2.1.2 beschriebene Risikoanalyse bestimmt die sicherheitstechnisch erforderlichen Integritätsklassen (Safety-Integrity-Levels) der einzelnen MSR-Sicherheitsfunktionen des Gesamtsystems. Für die Entwicklung der MSR-Sicherheitsfunktionen gilt es nun, die geforderte Systemintegrität anhand angemessener Methoden und Maßnahmen innerhalb eines sicherheitsgerechten Entwicklungsprozesses sicherzustellen. Dabei

Tabelle 5-2: *Systemarchitektur abhängig von der geforderten Systemintegrität (Safety-Integrity-Level SIL).*

Geforderte Integrität	Architektur	Verhalten/Bemerkung	Referenz
-/SIL1	1oo1	Integrität durch ausfallsichere Komponenten	-
SIL1/SIL2	1oo1D	integer (Fehler wird erkannt)	Bild 5-1
SIL2	1oo2	integer (typisch für ABS)	Bild 5-2
SIL2	2oo2	integer	Bild 5-3
SIL2/SIL3	1oo2D	fehlertolerant (Einfachfehler wird aufgefangen)	Bild 5-4
SIL3	2oo3	fehlertolerant (typisch für Steer-by-Wire)	Bild 5-5

ist zu berücksichtigen, welche Systeme unabhängig voneinander agieren bzw. sich gegenseitig beeinflussen können. Nur wenn eine gegenseitige Einflussnahme generell ausgeschlossen werden kann, ist eine separate Betrachtungsweise der einzelnen SIL möglich, andererseits müssen alle betroffenen Systeme nach dem höchsten in der Risikoanalyse ermittelten SIL entwickelt werden.

In **Bild 5-6** ist das angepasste Vorgehensmodell für die Entwicklung mechatronischer Systeme bei mobilen Arbeitsmaschinen dargestellt, welches den in diesem Bereich vorkommenden Integritätsstufen SIL1 bis SIL3 genügt. Die Entwicklungsschritte werden durch die Anwendung impliziter und expliziter Methoden und Maßnahmen, die anhand des erforderlichen SIL ausgewählt werden, bearbeitet.

Geprägt durch den standardmäßigen Aufbau mechatronischer Systeme in Sensorik, Aktorik und Informationsverarbeitung (siehe auch Bild 2-2) wird das V-Modell in zwei Teilen „Systementwicklung“ und „Softwareentwicklung“ aufgebaut. Die Entwicklungsmethoden und -maßnahmen des oberen Teils (Systementwicklung) zielen auf das komplette System bzw. Zusammenwirken untergeordneter Teilsysteme ab und behandeln Software als Black-Box-Element einzelner Systemkomponenten. Aus den Systemanforderungen werden die Funktionen spezifiziert, logisch verteilt und abschließend innerhalb der technischen Systemarchitektur festgeschrieben. Rekursionen auf Systemebene zwischen Testseite (rechts) und Spezifikationsseite (links) sollten aus Kostengründen strikt vermieden werden.

Der eigentliche Softwareentwicklungsprozess wird durch den unteren Teil des V-Modells vorgegeben. Die Softwareanforderungen werden analysiert, die Subsysteme und Module spezifiziert und in Serien-Code implementiert. Die Tests der Subsysteme, auch die Integrationstests des Seriensteuergeräts, ermöglichen hier zugelassene Rekursionen für eine Verbesserung der Spezifikation, da Spezifikations- und Testphase der Komponentenebene im Entwicklungsvorgang genügend nahe beisammen liegen.

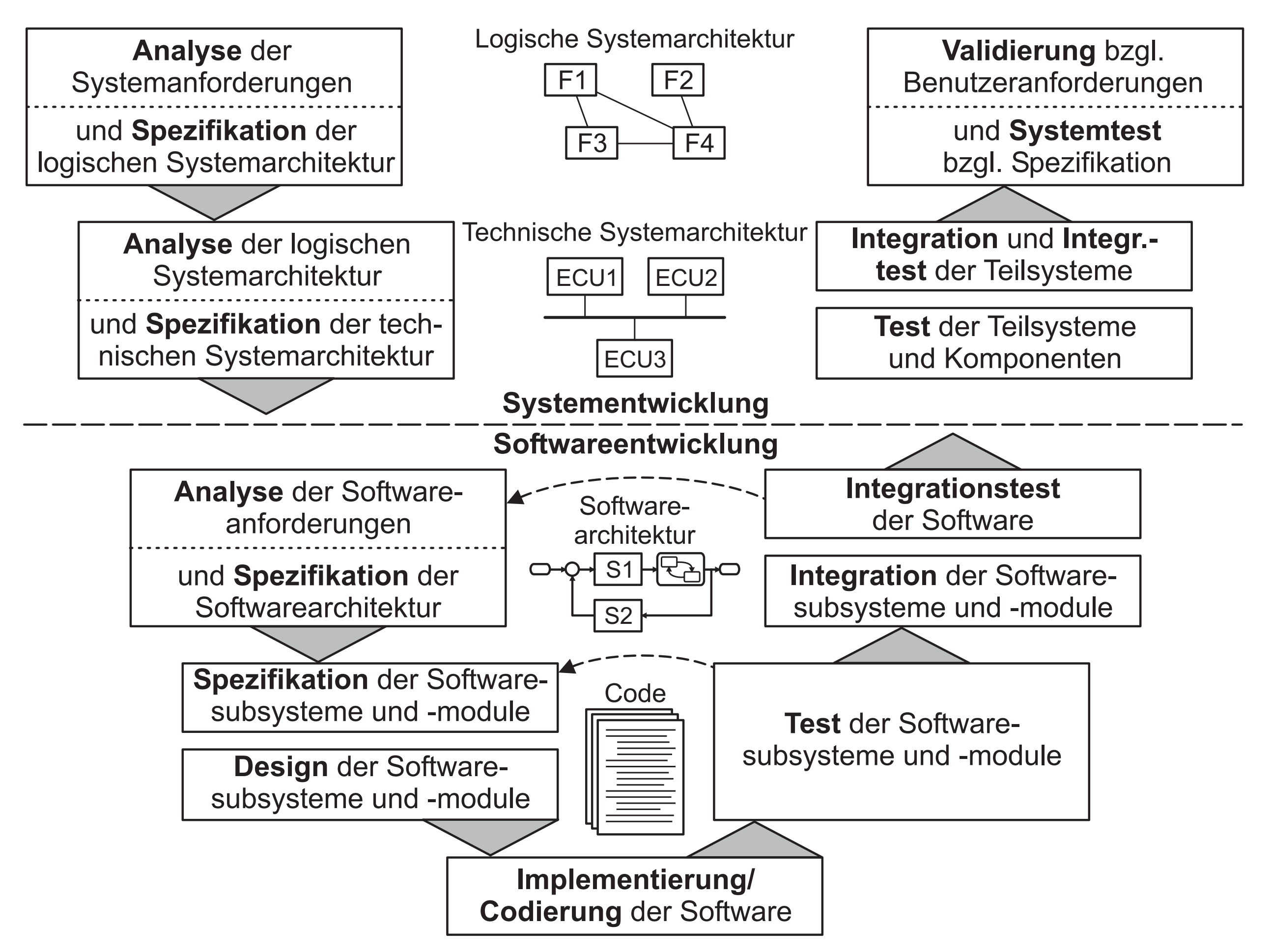


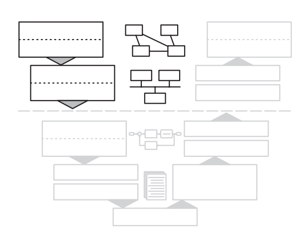
Bild 5-6: *Angepasstes V-Modell als Entwicklungsmodell für mechatronische Systeme mit Aufteilung in System- und Softwareentwicklung, Anregungen aus [190].*

5.3 Entwicklungsschritte mit Zuordnung der Methoden und Maßnahmen

In den folgenden Teilkapiteln sind die Entwicklungsschritte des V-Modells aus Kapitel 5.2 mit Zuordnung der explizit vorgeschlagenen Methoden beschrieben. Die jeweils zu Beginn aufgeführten Piktogramme zeigen, in welchem Bereich des Vorgehensmodells man sich befindet.

In den Tabellen zur Methodenzuordnung (Tabelle 5-3 bis 5-10) sind die Methoden und Maßnahmen abhängig vom geforderten Safety-Integrity-Level (SIL) empfohlen bzw. vorgeschrieben. Parallel wirkende Maßnahmen- und Methoden sind in Gruppen zusammengefasst und mit fortlaufenden Buchstaben (a, b, c, ...) gekennzeichnet. Zum Erlangen eines erforderlichen SIL ist es ausreichend, nur eine Maßnahme oder Methode aus diesen Gruppen auszuwählen. Alle anderen durchnummerierten Einträge sind eigenständig zu behandeln. Für weiterführende Informationen zu Methoden und Maßnahmen sind Referenzangaben in Form der Kapitelnummern oder Literaturstellen mit aufgeführt.

5.3.1 Analyse und Spezifikation der Systemanforderungen und -architektur

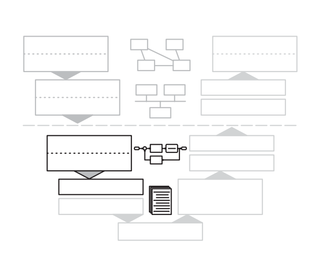


Die ersten beiden Schritte des V-Modells analysieren die Systemanforderungen und bestimmen die Spezifikation der Teilsysteme bzw. des Gesamtsystems. Die festgelegten Funktionen werden logisch verknüpft und in die sicherheitsgerechte technische Systemarchitektur, bestehend aus dem vernetzten Layout der erforderlichen Steuerrechner und Komponenten, überführt. In **Tabelle 5-3** sind explizite Maßnahmen bzw. Methoden aufgezählt, die in diesen Entwicklungsschritten relevant sind. Pflicht für alle Integritätsstufen sind konventionelle bzw. modellbasierte Methoden zur Lastenhefterstellung und die für die Bestimmung des Risikopotenzials (Bestimmung des SIL) notwendige Risikoanalyse. Die für höhere Sicherheitsanforderungen (SIL-Werte) dringend empfohlene System-FMEA bildet eine wichtige Säule des sicherheitsgerechten Entwicklungskonzepts und begleitet die gesamte Spezifikationsphase.

Tabelle 5-3: *Entwicklungsschritt:* ***Analyse und Spezifikation der Systemanforderungen und -architektur****. Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL.*

Methode/Maßnahme (Systemanalyse und -spezifikation)		Referenz	SIL1	SIL2	SIL3
1a	Lastenheft/Anforderungsanalyse/Pflichtenheft	[169]	DE	DE	DE
1b	Modellbasierte Spezifikation (simulationsgestütztes, modellbasiertes Lastenheft)	4.3.1	DE	DE	DE
2	Systemstrukturanalyse (Signalflussplan, Schnittstellenanalyse)	4.2.1.1	DE	DE	DE
3	Risikoanalyse (Ermittlung des notwendigen SIL)	4.2.1.2	DE	DE	DE
4	System-FMEA	4.2.1.3	E	DE	DE
5	Komponenten-FMEA	4.2.1.3	-	E	DE
6	Fehlerbaumanalyse (FTA)	[168]	E	E	DE

5.3.2 Analyse und Spezifikation der Softwareanforderungen und -architektur



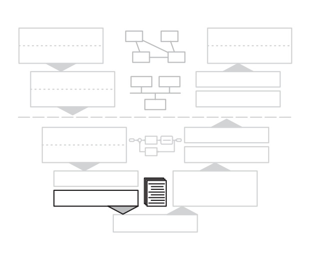
Liegt die technische Systemarchitektur fest, wird das Lastenheft des jeweiligen elektronischen Steuergeräts softwaretechnisch analysiert und umgesetzt. Aus den funktionellen Anforderungen für das Steuergerät wird die Spezifikation der Softwaresubsysteme und -module abgeleitet. Wie auch bei der Systemspezifikation sind die Methoden zur Erstellung der Softwarelastenhefte nach **Tabelle 5-4** für alle Integritäts-Levels dringend empfohlen. Der Anwendungsbereich der in dieser Arbeit favorisierten System-

FMEA verschiebt sich in diesem Entwicklungsschritt in Richtung sicherheitstechnische Untersuchung von Softwaremodulen und ihrer Komponenten.

Tabelle 5-4: *Entwicklungsschritt:* ***Analyse und Spezifikation der Softwareanforderungen und -architektur****. Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL.*

Methode/Maßnahme (SW-Analyse und SW-Spezifikation)		Referenz	SIL1	SIL2	SIL3
1a	Lastenheft/Anforderungsanalyse/Pflichtenheft	[169]	DE	DE	DE
1b	Modellbasierte Spezifikation (simulationsgestütztes, modellbasiertes Lastenheft)	4.3.1	DE	DE	DE
2	System-FMEA	4.2.1.3	E	DE	DE
3a	Komponenten-FMEA (Software-FMEA)	4.2.1.3	E	E	DE
3b	Fehlerbaumanalyse (FTA)	[168]	E	E	DE
3c	Software-Criticality-Analysis (SCA)	[171, 172]	E	E	DE
4	Strukturierte Analyse	4.2.1.4	E	E	DE
5a	Zustandsdiagramme	[151]	-	E	DE
5b	Entscheidungstabellen/Wahrheitstabellen	[151]	-	E	DE
6	Model-in-the-Loop	4.3.2	E	E	E
7	Rapid-Control-Prototyping	4.3.3	-	E	E
8	SW-Audit (ISO 15504, SPICE)	2.3.2	-	E	DE

5.3.3 Design der Softwaresubsysteme und -module

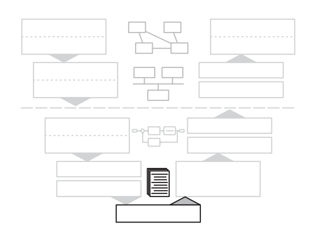


Das Softwaredesign setzt die Spezifikationsdaten der Software in für die Implementierung und Codierung verwertbare Informationen um. Der Fokus liegt dabei auf der strukturellen Gestaltung der Subsysteme und Module als Basis für die nachfolgende Umsetzung in Serien-Code. **Tabelle 5-5** beinhaltet die Methodenzuordnung für diesen Entwicklungsschritt. Herausragende Punkte sind die Verwendung erprobter Komponenten und die Wiederverwendbarkeit. Um Sicherheit und Qualität hochzuhalten, sollten grundsätzlich erprobte Hardware- und Softwarekomponenten da eingesetzt werden, wo Neuentwicklungen eingespart werden können. Gerade bei der Softwareentwicklung ist der Aspekt der Wieder- und Weiterverwendung von bereits implementierten Funktionen leicht zu bewerkstelligen und fördert die Zuverlässigkeit der Systeme bei geringerem Entwicklungsaufwand. Eine durchgängig modellbasierte Entwicklungskette erleichtert hierbei den Zugriff auf schon entwickelte Modelle. Bei stark sicherheitskritischen Systemen sollten Vorkehrungen zur Fehlererkennung und Diagnose getroffen werden. Die EN 61508 [151] liefert dazu mögliche Konzepte und Anleitungen.

Tabelle 5-5: *Entwicklungsschritt:* ***Design der Softwaresubsysteme und -module****. Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL.*

Methode/Maßnahme (Softwaredesign)		Referenz	SIL1	SIL2	SIL3
1	Erprobte Hardware/Software	[151]	E	DE	DE
2	Wiederverwendbarkeit von SW-Modulen/Funktionen	[151]	E	DE	DE
3	Strukturierte Analyse	4.2.1.4	E	E	DE
4a	Zustandsdiagramme	[151]	-	E	DE
4b	Entscheidungstabellen/Wahrheitstabellen	[151]	-	E	DE
5	Fehlererkennung und Diagnose	[151]	-	DE	DE
6a	Vorsehen einer externen Überwachung (Guardian)	[151]	E	E	E
6b	Software Diversität	[151]	E	E	E
6c	Priorisierung von Sicherheitsfunktionen innerhalb SW	[151]	E	E	E
6d	Fehlerbeherrschungsprinzipien von Software	[151]	E	E	E
7	Model-in-the-Loop	4.3.2	E	E	E
8	Rapid-Control-Prototyping	4.3.3	-	E	E
9	Konfigurationsmanagement	4.2.1.4	-	E	DE
10	SW-Audit (ISO 15504, SPICE)	2.3.2	-	E	DE

5.3.4 Implementierung und Codierung der Software

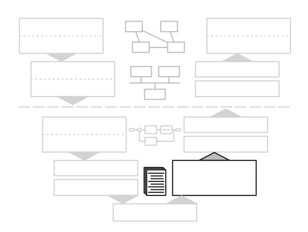


Die eigentliche Implementierung der Software geschieht mittels konventioneller manueller Umsetzung des Softwaredesigns in Serien-Code oder über automatische Code-Generierung direkt aus dem Simulationsmodell im Falle einer durchgängigen modellbasierten Entwicklung. Das Ergebnis dieses Entwicklungsschritts ist der nach Spezifikation programmierte Steuergeräte-Code, der im kompilierten Zustand direkt auf die Ziel-Hardware geladen werden kann. Die Verwendung von zertifizierten **oder** erprobten Werkzeugen und höheren Programmiersprachen ist für eine sicherheitsgerechte Entwicklung unerlässlich. Die Anwendung von Softwarestandards, die zwar den möglichen Leistungsumfang einer Sprache einschränken, fehleranfällige Konstrukte aber nicht mehr zulassen, befindet sich in immer weiterer Verbreitung. Nach **Tabelle 5-6** wird die Einhaltung von SW-Standards erst ab SIL3 vorgeschrieben, grundsätzlich aber auch für niedrigere Safety-Integrity-Levels empfohlen.

Tabelle 5-6: *Entwicklungsschritt:* ***Implementierung/Codierung der Software****. Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL.*

Methode/Maßnahme (SW-Implementierung/Codierung)		**Referenz**	**SIL 1**	**SIL 2**	**SIL 3**
1	Wiederverwendbarkeit von SW-Modulen/Funktionen	[151]	E	DE	DE
2	Zertifizierte **oder** erprobte Werkzeuge	-	DE	DE	DE
3	Höhere Programmiersprachen	-	DE	DE	DE
4a	Zustandsdiagramme	[151]	-	E	DE
4b	Entscheidungstabellen/Wahrheitstabellen	[151]	-	E	DE
5	Programmierung nach SW-Standards (z. B. MISRA)	4.2.1.4	E	E	DE
6	Model-in-the-Loop	4.3.2	E	E	E
7	Automatische Code-Generierung	4.3.5	-	E	E
8	Konfigurationsmanagement	4.2.1.4	-	E	DE
9	SW-Audit (ISO 15504, SPICE)	2.3.2	-	E	DE

5.3.5 Test der Softwaresubsysteme und -module

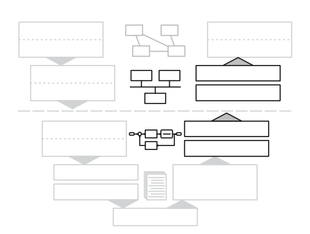


Aufgabe des ersten Entwicklungsschritts der Testseite des V-Modells ist die Überprüfung der korrekten Softwareumsetzung der Funktionen auf Modulebene. Standardmethoden, wie Funktionstest oder Black-Box-Test sind obligatorisch und müssen in jedem Fall vorgesehen werden, siehe **Tabelle 5-7**. Bei konventioneller Vorgehensweise stehen statische Analysen und dynamische Tests im Mittelpunkt der Verifikation und werden für Systeme ab SIL2 dringend empfohlen. Als modellbasierte Variante ist der Software-in-the-Loop-Test eine effektive Methode, den programmierten Code noch ohne Zielhardware auf Funktionalität und Fehlerverhalten zu untersuchen.

Tabelle 5-7: *Entwicklungsschritt:* ***Test der Softwaresubsysteme und -module****. Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL.*

Methode/Maßnahme (Test der SW-Subsysteme, -Module)		**Referenz**	**SIL 1**	**SIL 2**	**SIL 3**
1a	Funktionstest	4.2.2.2	DE	DE	DE
1b	Black-Box-Test	4.2.2.2	DE	DE	DE
2	Probalistischer Test	[151]	-	E	E
3	Statische Analyse und Test	4.2.2.2	E	DE	DE
4	Dynamische Analyse und Test	4.2.2.2	E	DE	DE
5	Schnittstellentest	4.2.2.2	E	E	DE
6	Performance-Test	4.2.2.2	E	E	DE
7	Software-in-the-Loop	4.3.4	-	E	E

5.3.6 Integrationstests der Software und Teilsysteme, Komponententests



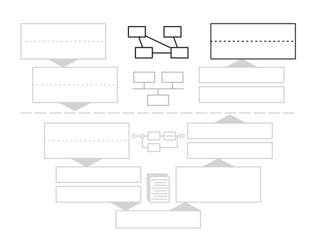
Der breiteste Anwendungsbereich von Entwicklungstests gliedert sich in Komponenten- und Integrationstests. **Komponententests** bzw. Tests von Teilsystemen verifizieren das korrekte Verhalten der Komponente bezüglich ihrer Spezifikationsanforderungen und können über Black-Box-Test, Funktionstest oder auch statische und dynamische Analyse (dann hauptsächlich im Anwendungsfall auf Software) durchgeführt werden.

Die **Integrationstests** prüfen das zu integrierende System bezüglich der Spezifikation der technischen Systemarchitektur und reichen von der Eingliederung der Softwaremodule in das Softwareprojekt (Tests auf die korrekte Softwarearchitektur) bis zur Integration der einzelnen Teilsysteme, wie elektronische Steuergeräte, Sensorik oder Aktorik, in das Gesamtsystem. Getestet wird Schnittstellenverhalten, Kommunikation, Koordination und Zeitverhalten im realen Systemverbund oder als Komponente in der virtuellen Abbildung des Systemumfelds, z. B. mittels Hardware-in-the-Loop. In **Tabelle 5-8** sind die wichtigsten Testmethoden für diesen Entwicklungsschritt aufgeführt.

Tabelle 5-8: *Entwicklungsschritt:* ***Integrationstest und Komponententest****. Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL.*

Methode/Maßnahme (Integrationstest, Komponententest)		Referenz	SIL 1	SIL 2	SIL 3
1a	Funktionstest	4.2.2.2	DE	DE	DE
1b	Black-Box-Test	4.2.2.2	DE	DE	DE
2	Probalistischer Test	[151]	-	E	E
3	Statische Analyse und Test	4.2.2.2	E	DE	DE
4	Dynamische Analyse und Test	4.2.2.2	E	DE	DE
5	Software-in-the-Loop	4.3.4	-	E	E
6a	Hardware-in-the-Loop	4.3.6	-	E	DE
6b	Labortest im Brettaufbau	4.2.2.2	-	E	DE
7	Prüfstandsversuche	4.2.2.1	E	E	E
8	EMV-, Umwelt-, Vibrationstest	4.2.2.1	E	DE	DE
9	Datenaufzeichnung und -analyse	4.2.2.2	E	DE	DE

5.3.7 Systemtest und Validierung

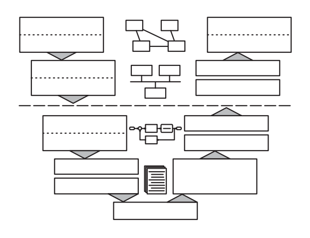


Im letzten Entwicklungsschritt vor der Freigabe steht der Systemtest und nachfolgend die eigentliche Validierung des Systems bezüglich der Benutzeranforderungen. Der **Systemtest** erprobt das Gesamtsystem gezielt anhand der Spezifikationsanforderungen der logischen Systemarchitektur. Im Gegensatz zu den vorangegangenen Verifikationsmaßnahmen, die jeweils die Resultate einer Entwicklungsphase auf Spezifikation und Vorgaben überprüfen, steht die **Validierung** für die Abnahme eines Produkts hinsichtlich seines Einsatzzwecks und der Benutzererwartungen. **Tabelle 5-9** zeigt empfohlene und dringend empfohlene Methoden, die in diesem Entwicklungsschritt ihre Anwendung finden.

Tabelle 5-9: *Entwicklungsschritt:* ***Systemtest und Validierung****. Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL.*

	Methode/Maßnahme (Systemtest und Validierung)	Referenz	SIL 1	SIL 2	SIL 3
1	Probalistischer Test	4.2.2.2	-	E	E
2	Tests im breiten Anwendungsfeld	4.2.2.1	E	E	E
3	Systemtest	4.2.2.1	DE	DE	DE
4	EMV-, Umwelt-, Vibrationstest	4.2.2.1	E	DE	DE
5	Test der Funktionalität	4.2.2.1	DE	DE	DE
6	Test des Fehlerverhaltens	4.2.2.1	DE	DE	DE

5.3.8 Universelle Maßnahmen für die gesamte Entwicklung



Die in **Tabelle 5-10** genannten Maßnahmen und Methoden sollen den gesamten Entwicklungsvorgang begleiten. Die meisten davon sind für ein sicherheitsgerechtes Systemverhalten, aber auch für geforderte Qualitätsmaßstäbe, unerlässlich. Einer der wichtigsten Punkte ist das durchgängige Prozessmanagement in Verbindung mit der lückenlosen Dokumentation der Entwicklung. Erst dadurch können die getroffenen sicherheitstechnischen Maßnahmen hinsichtlich Systemeigenschaften und Entwicklungsprozess im Falle einer möglichen Beweispflicht durch Gewährleistung oder Produkthaftung nachgewiesen werden. Einige vorgestellte Methoden implizieren bereits eine umfassende Dokumentation bei ihrer Anwendung (System-FMEA, Fehlerbaumanalyse), andere schreiben dieses explizit vor (z. B. einige Programmierstandards).

Tabelle 5-10: *Auswahl von empfohlenen (E) und dringend empfohlenen (DE) Entwicklungsmethoden und -maßnahmen in Abhängigkeit des geforderten SIL, welche die* ***gesamte Entwicklung*** *begleiten.*

	Methode/Maßnahme (gesamte Entwicklung)	Referenz	SIL 1	SIL 2	SIL 3
1	Dokumentation	[151]	DE	DE	DE
2	Prozessmanagement	2.3	DE	DE	DE
3	Projektmanagement	-	DE	DE	DE
4	Qualitätsmanagement	-	DE	DE	DE
5	Erprobte Komponenten, Subsysteme, Systeme	[151]	DE	DE	DE
6	Erprobte Methoden, Werkzeuge, Prozesse	[151]	DE	DE	DE
7a	Computerunterstützte Werkzeuge	[151]	E	E	E
7b	Checklisten	[151]	E	E	E
7c	Sonstige formale Methoden	[151]	E	E	E

6 Anwendungsbeispiel „Gerät steuert Traktor“ mit Vorgewendeautomatik

Ein wichtiger Prüfstein für die Erarbeitung eines sicherheitsgerechten Entwicklungskonzepts ist die Weiterentwicklung und Untersuchung eines aussagekräftigen Versuchsträgers in Theorie und Praxis. Für die Auswahl eines geeigneten Maschinensystems wurden verschiedene Kriterien herangezogen: Aufbauend auf eine praxisnahe Anwendung sollte Potenzial für zusätzliche Automatisierungen und Mechatroniken vorhanden sein. Das Maschinensystem sollte als ein typisches Beispiel für den Bereich der mobilen Arbeitsmaschinen gelten. Eigenheiten, wie Kombination von komplexen Arbeitsprozessen mit Fahrfunktionalität, Verwendung unterschiedlicher Leistungsschnittstellen mit verschiedenen Technologien und systemübergreifende Funktionalität, standen dabei im Vordergrund. Die Realisierung zusätzlicher Automatiken, speziell unter Einbeziehung sicherheitsrelevanter Systeme, sollte dazu beitragen, Vorgehen, Methoden und Entwicklungsmaßnahmen anzupassen und im Anschluss das erarbeitete Entwicklungskonzept zu verifizieren.

Im ersten Teil dieses Kapitels werden Systemstruktur, elektronische Ausrüstung des Versuchsgespanns und Logik der entwickelten Automatiken vorgestellt. Nach der Beschreibung der durchgeführten System- und Risikoanalysen des Anwendungsbeispiels befasst sich der darauf folgende Abschnitt mit ausgewählten Teilsystemen, welche die sicherheitsgerechte Entwicklung des Versuchsträgers verdeutlichen.

6.1 Systembeschreibung und Aufbau der Automatiken

6.1.1 Versuchsträger und Elektronikkonzept

Für die Untersuchung der funktionalen Sicherheit mobiler Arbeitsmaschinen wurde die in **Bild 6-1** dargestellte Traktor/Geräte-Kombination aus Traktor mit Ringpacker im Frontanbau und Kreiselegge mit pneumatischer Drillmaschine im Heckanbau ausgewählt. Die Maschinen wurden großzügiger Weise von den Firmen ACGO-Fendt und Lemken für den



Bild 6-1: *Automatisierte Traktor/Geräte-Kombination als Versuchsträger bei der Arbeit.*

gesamten Zeitraum des Forschungsprojekts zur Verfügung gestellt. Für erweiterte Funktionen und zusätzliche Systemzustände wurde eine Drillmaschine mit eigenem Fahrwerk ausgewählt, die zur Verkürzung des Hebelarms beim Ausheben hydraulisch auf die Kreiselegge aufgesattelt wird. **Tabelle 6-1** zeigt die wichtigsten technischen Daten des Versuchsgespanns.

Tabelle 6-1: *Technische Daten des Versuchsgespanns.*

Traktor	
Typ	Fendt Favorit 716
Motor	6 Zyl., Turbo, Hubraum 5703 cm^3
Leistung (ECE)	118 kW (160 PS)
Getriebe	stufenlos, hydrostatisch-mechanisch leistungsverzweigt
Leergewicht	6050 kg
Radstand	2700 mm
Bereifung vorne Bereifung hinten	540/65 R 28 650/65 R 38
Landwirtschaftliche Geräte (Arbeitsbreite 3 m)	
Ringpacker	Lemken Variopack 110 WDP 70, Gewicht 758 kg
Kreiselegge	Lemken Zirkon 7/300, Gewicht 1192 kg, Antrieb über Zapfwelle
Drillmaschine	Lemken Solitär 9, pneumatische Saatverteilung, auf Kreiselegge aufsattelbar, Leergewicht 930 kg

Für die Realisierung automatisierter Zugriffe auf die Traktorfunktionen hinsichtlich Antriebsstrang und Geräteschnittstellen musste die Standardelektronik des Traktors modifiziert werden. Da die wichtigsten Funktionen des Favorit 716 über eine zentrale Mensch-Maschine-Schnittstelle (Multifunktionsarmlehne) elektronisch angesprochen werden, konnte hier die geeignete Schnittstelle für eine zusätzliche Elektronik gefunden werden. Wie in **Bild 6-2** gezeigt, wurde der Kabelstrang zwischen Fahrzeugrechner und Multifunktionsarmlehne aufgebrochen und ein Rapid-Control-Prototyping-Rechner (MicroAuto-Box, Fa. dSPACE) integriert. Dieses RCP-Werkzeug, das als Traktorrechner im Sinne der ISO 11783 arbeitet, ist somit in der Lage, die Funktionen der Multifunktionsarmlehne (Getriebeverstellung, Neutralschaltung, Betätigung der hydraulischen Zusatzventile und des Heckhubwerks) für den Traktor zu generieren und außerdem Ein-

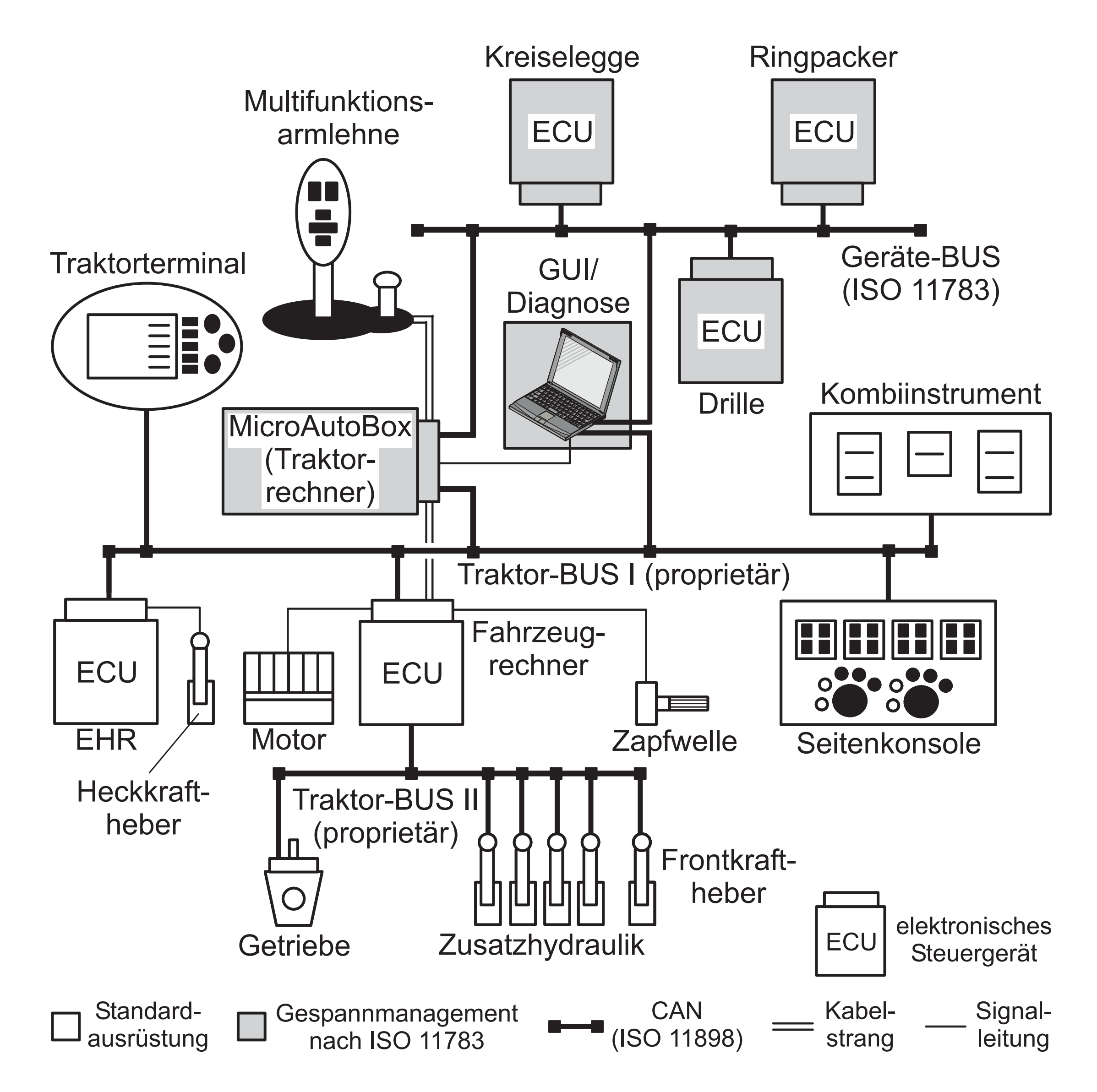


***Bild 6-2:** Elektronikarchitektur des automatisierten Versuchsgespanns.*

griffe des Fahrers zu diagnostizieren. Die restlichen Traktorfunktionen (Fronthubwerk, Konfiguration der Zusatzventile und Heckzapfwelle) werden über an die Traktorspezifikation angepasste CAN-Botschaften auf dem Traktor-BUS I abgerufen.

Die landwirtschaftlichen Geräte wurden mit eigenen elektronischen Steuergeräten (Typ ESX 2, Fa. Sensor-Technik Wiedemann, Basis Infineon C167) ausgerüstet und sind über einen separaten CAN-Geräte-BUS in das Konzept eingebunden. Die Auslegung dieses CAN-Netzwerks ist zur Normung ISO 11783 [117] weitestgehend konform, mit der Ausnahme fest zugewiesener Teilnehmeradressen ohne automatische Adressvergabe. Mit zwei unabhängigen CAN-Controllern fungiert der Traktorrechner (MicroAutoBox) als Brückenrechner zwischen Geräte-BUS und Traktor-BUS I und stellt somit die Kommunikation zwischen Traktor und Geräten sicher.

Die Programmierung der elektronischen Steuergeräte des Gespanns basiert auf zwei unterschiedlichen Vorgehensweisen, nach konventioneller Umsetzung in C-Code und graphischer Programmierung mit Matlab/Simulink/Stateflow. Für die Steuerrechner der landwirtschaftlichen Geräte wurden frei programmierbare Steuereinheiten ausgewählt, deren Programmierung mit der Hochsprache C manuell bewerkstelligt wird. Die Ein- und Ausgänge sowie weitere spezielle Funktionen werden über ein steuergeräteeigenes Betriebssystem (BIOS) angesprochen.

Da die größten Anforderungen im Versuchsgespann bezüglich Funktionalität und Rechenleistung auf den Traktorrechner fallen, war hier die Verwendung einer besonderen, leistungsfähigen Entwicklungshardware hilfreich. Mit dem ausgewählten RCP-Werkzeug „MicroAutoBox“ war es möglich, die im MIL-Test entwickelten Reglerstrukturen in der graphischen Programmierung mit Matlab/Simulink/Stateflow direkt weiter zu verwenden. Zusätzlich brachte die Online-Zugriffsmöglichkeit auf sämtliche Variablen der MicroAutoBox-Logik in Echtzeit erhebliche Vorteile für Entwicklung und Diagnose mit sich.

6.1.2 Messdatenerfassung

Als Benutzerschnittstelle (Graphical User Interface GUI), Diagnosewerkzeug und für den Zugriff auf in Echtzeit erfassbare oder abgespeicherte Messdaten steht ein Mess-Laptop zur Verfügung. Es ermöglicht die Online-Bedienung der MicroAutoBox über die zugehörige Software ControlDesk und ist über die CAN-Diagnose-Software CANalyzer in die beiden CAN-Netzwerke integriert. In **Bild 6-3** ist der genaue Aufbau der Datenflüsse für die Messdatenerfassung gezeigt. Die sensorisch erfassten Messwerte sowie die wichtigsten Signale der CAN-Kommunikation werden in einem nicht flüchtigen Flash-Speicher (Ringpuffer) der MicroAutoBox zwischengespeichert und können über die Host-Schnittstelle auf das Mess-Laptop ausgelesen werden.

Während die diskreten Daten der traktorseitigen Sicherheitssensorik direkt über die Eingänge der MicroAutoBox erfasst werden, liegt die Verarbeitung der sicherheitsrelevanten Sensordaten der Geräte im Aufgabenbereich der jeweiligen Geräterechner. Die aufbereiteten Signale werden daraufhin auf dem Geräte-BUS für den Traktorrechner und die anderen Geräterechner zur Verfügung gestellt. **Tabelle 6-2** nennt die sensorische Zusatzausrüstung für Traktor und Geräte, **Bild 6-4** zeigt die entsprechende Lokalisierung im Gespann mit korrespondierender Nummerierung.

6.1.3 Aufbau der Automatiken

Mit der elektronischen Erweiterung des Versuchsgespanns konnten zwei neuartige Automatiken implementiert werden. Zum einen wurde ein vollständiges Vorgewende- und Rei-

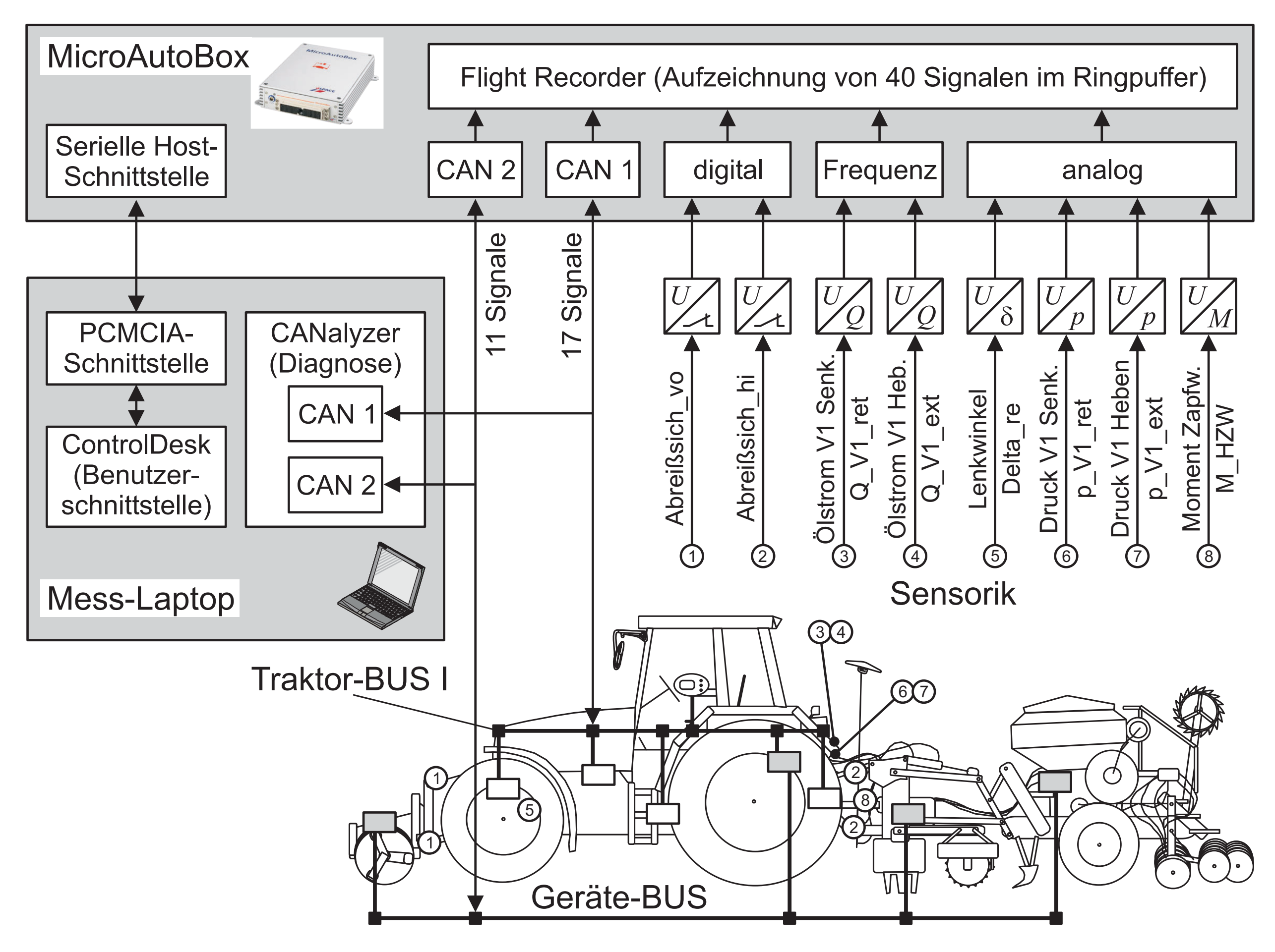


Bild 6-3: *Datenflüsse für Aufzeichnung und Diagnose der Messgrößen des Versuchsgespanns mit Sicherheitssensorik des Traktorrechners. Anmerkung: Die Abreißsicherungen benötigen jeweils drei Kanäle (Oberlenker, Unterlenker links und rechts).*

henmanagement auf Basis geräteseitiger Traktorsteuerungen realisiert, welches über verteilte Funktionalitäten der Geräterechner den Traktor hinsichtlich Geschwindigkeit und elektrischer, mechanischer sowie hydraulischer Schnittstellen regelt. Zum anderen wurde eine Prozessautomatisierung des Traktorrechners entwickelt, die den automatischen Wendevorgang am Vorgewende hinsichtlich der Längsführung des Traktor/Geräte-Gespanns ohne aufwendige Navigation oder Sensorik ermöglicht.

„Gerät steuert Traktor“ mit Reihenautomatik

Im Rahmen des Projekts „Prozesssicherheit Landmaschinenelektronik“ wurde in einer parallel entstandenen Forschungsarbeit [7] speziell das Automatisierungspotenzial mobiler Arbeitsmaschinen untersucht und anhand eines Beispiels für geräteseitige Traktorsteuerungen behandelt. Freimann konzipierte und realisierte in dieser Arbeit ein vollautomatisiertes Vorgewendemanagement, um den Fahrer beim Einsetzen und Ausheben der Geräte erheblich zu entlasten. In der implementierten Automatik übergibt der Fahrer durch einen einzigen Knopfdruck den gewünschten örtlichen Arbeitsbeginn bzw. Aushubpunkt an das

Tabelle 6-2: *Sensorische Zusatzausrüstung des Versuchsträgers. Die Tabelle dient zugleich als Legende zu Bild 6-4. (⊥ = induktiver Näherungsschalter)*

Nr.	Signal	Prinzip	Nr.	Signal	Prinzip
Traktor			13	Abreißsicherung zur Drille (3x)	⊥ $\rightarrow U$
1	Ist-Geschwindigkeit (Radar)	$f \rightarrow U$	14	Position Gelenkwelle	⊥ $\rightarrow U$
2	Drehzahl HZW	$f \rightarrow U$	**Drillmaschine**		
3	Drehmoment HZW	$M \rightarrow U$	15	Drehzahl Gebläse	$f \rightarrow U$
4	Lenkwinkel (rechtes Rad)	$\delta \rightarrow U$	16	Drehzahl Saatgutwelle	$f \rightarrow U$
5	Druck Ventil 1 (extend, retract)[a)]	$p \rightarrow U$	17	Drehzahl Sponrad	$f \rightarrow U$
6	Ölstrom Ventil 1 (ext., retr.)[a)]	$Q \rightarrow U$	18	Status Fahrgassenschaltung	$I \rightarrow U$
7	Abreißsicherung FKH (3x)	⊥ $\rightarrow U$	19	Position Treppe	⊥ $\rightarrow U$
8	Abreißsicherung HKH (3x)	⊥ $\rightarrow U$	20	Position Deckel Saatkasten	⊥ $\rightarrow U$
Kreiselegge			21	Füllstand Saatkasten	⊥ $\rightarrow U$
9	Position Aufsattelung (2x)[b)]	$\alpha \rightarrow U$	**Ringpacker**		
10	Drehzahl Messerkreisel	$f \rightarrow U$	22	Drehzahl Ringe	$f \rightarrow U$
11	Drehzahl Andruckwalze	$f \rightarrow U$	23	Position Stütze	⊥ $\rightarrow U$
12	Position Spuranreißer (li., re.)	⊥ $\rightarrow U$	24	Lenkanschlag (links, rechts)	⊥ $\rightarrow U$

a) Zwei Kanäle: Heben und Senken
b) Zwei redundante Kanäle

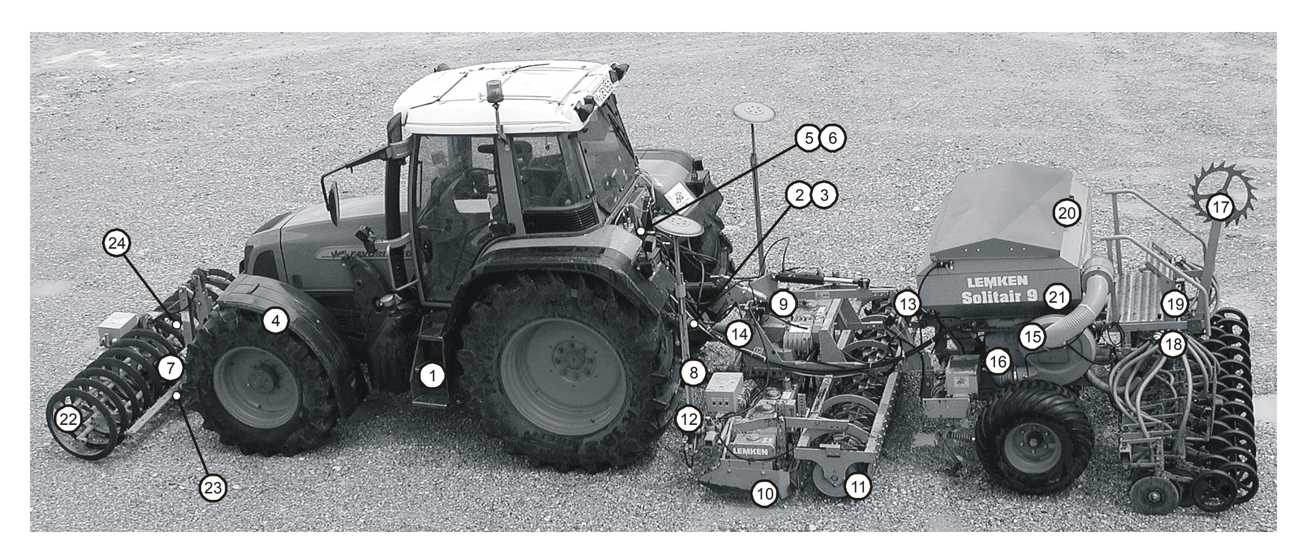


Bild 6-4: *Sensorische Zusatzausrüstung des Versuchsgespanns.*

System. Die Geräte verarbeiten diesen Wert mit den geometrischen Daten und aktuellen Systemparametern und regeln den Traktor in Fahrgeschwindigkeit und zugewiesenen Schnittstellen so, dass sie die eigene Arbeit genau am Applikationspunkt beginnen bzw. beenden können. Das Prinzip „Gerät steuert Traktor“ unterscheidet sich damit grundsätzlich von den im Stand der Technik beschriebenen zeit-, weg- oder ereignisgelenkten Ablaufsteuerungen. Im weiteren Ansatz wurde die Automatik von Freimann durch eine autonome Prozessführung an der Kreiselegge beim Reihefahren erweitert. Diese erfolgt

durch Regelung des Drehmoments an der Heckzapfwelle mit der Fahrgeschwindigkeit als Stellgröße. Für detaillierte Informationen sei auf [7] verwiesen. Die zusammen mit Freimann entwickelten Automatiken wurden daraufhin in zahlreichen Funktionsversuchen optimiert und mit umfangreichen Sicherheitsabfragen erweitert, um eine geeignete Versuchsplattform in Bezug auf Entwicklung, Verifikation und Validierung von MSR-Sicherheitsfunktionen zu schaffen.

Für die Realisierung des Prinzips „Gerät steuert Traktor“ konnte der Traktorrechner Befehle bezüglich Soll-Geschwindigkeit und Traktorschnittstellen aus dem Geräte-BUS annehmen, verarbeiten und entsprechend seiner Strategie an die Energiequelle Traktor weitergeben, wofür er nach ISO 11783, Teil 9 mit der Klasse 3 spezifiziert wurde. In **Bild 6-5** sind die logischen Zusammenhänge und Aufgaben der automatisierten Teilsysteme gezeigt.

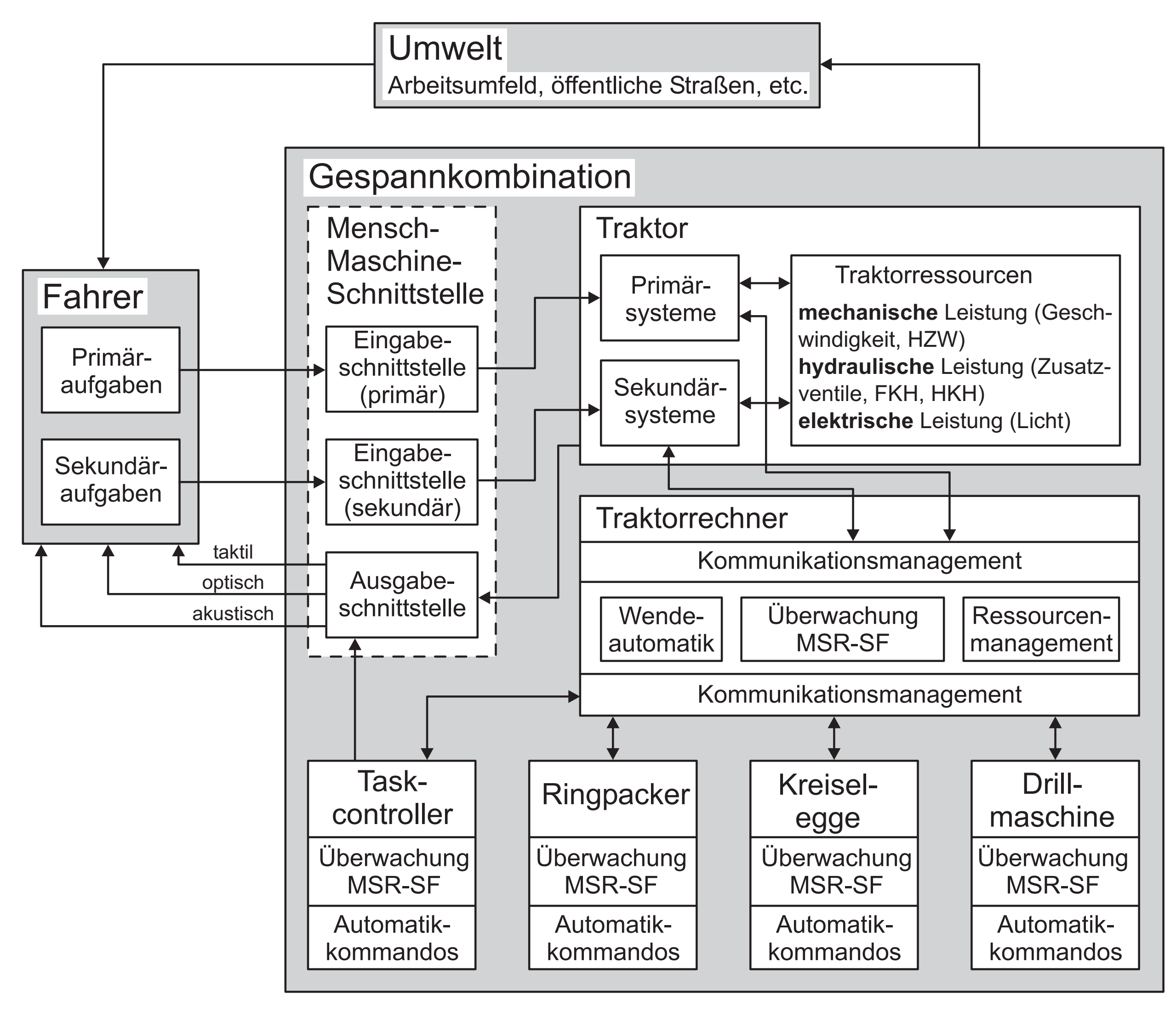


Bild 6-5: *Interaktionen und logische Verknüpfung der Teilsysteme im automatisierten Traktor/Geräte-Gespann für die Realisierung der geräteseitigen Traktorkommandos und der Wendeautomatik.*

Steuerung und Konfiguration der Automatiken sowie wichtige Applikationseinstellungen erledigt der Fahrer über die, um die Darstellung des Taskcontrollers erweiterte, Mensch-Maschine-Schnittstelle (z. B. gewünschtes Geschwindigkeitslimit, Fahrgassenschaltung, erforderliche Saatmenge, etc.). Die Automatiken entlasten den Fahrer sowohl in einigen seiner Primäraufgaben, wie Schaltung der Hubwerke, der hydraulischen Ventile oder Einregeln der korrekten Fahrgeschwindigkeit, wie auch bei Sekundäraufgaben, z. B. Konfiguration des Ölstroms, Hubhöhenbegrenzung oder anderen Einstellungen, die nun automatisch von den Geräten getroffen werden. Die Funktionen werden zum einen direkt in den Geräterechnern auf Sinnhaftigkeit der angeforderten Traktorressource[1)] überprüft, zum anderen zentral im Traktorrechner vor Generierung des eigentlichen Befehls an den Traktor überwacht. In **Tabelle 6-3** sind die Zugriffe auf freigegebene Traktorressourcen, d. h. Konfigurationseinstellungen, Betätigungen und Geschwindigkeitsvorgaben aufgelistet, die für die Automatikkommandos der Geräte und des Taskcontrollers an den Traktorrechner notwendig sind.

Tabelle 6-3: *Zugriffe der Geräte und des Taskcontrollers auf Traktorressourcen bei der Automatisierung „Gerät steuert Traktor“.*

Traktorressource	Traktorressource
Anforderung durch die Kreiselegge	Ölstrom Ventil 1 (Aufsattelung) Q_{V1}
Soll-Geschwindigkeit v_{soll_Egge}	Status Ventil 1 (Aufsattelung)
Maximalgeschwindigkeit v_{max_Egge}	Ölstrom Ventil 2 (Gebläse) Q_{V2}
Ölstrom Ventil 3 (Spuranreißer) Q_{V3}	Status Ventil 2 (Gebläse)
Status Ventil 3 (Spuranreißer)	Elektrische Leistung (Beleuchtung)
Hubposition Heckkraftheber	**Anforderung durch den Ringpacker**
Übersetzungsstufe Heckzapfwelle	Soll-Geschwindigkeit v_{soll_Packer}
Status Heckzapfwelle	Maximalgeschwindigkeit v_{max_Packer}
Anforderung durch die Drillmaschine	Hubposition Frontkraftheber
Soll-Geschwindigkeit v_{soll_Drille}	**Anforderung durch den Taskcontroller**
Maximalgeschwindigkeit v_{max_Drille}	Maximalgeschwindigkeit v_{max_Task}

Der zusätzliche Informationsaustausch zwischen den Geräterechnern, dem Traktorrechner und dem Taskcontroller wird ebenfalls über den Geräte-BUS abgewickelt. Neben den Automatikkommandos werden so die gewonnenen Daten der Sicherheitssensorik und andere standardmäßig erfasste Systemparameter kommuniziert.

1) Der Begriff „Ressource“ beschreibt die Verfügbarkeit von Funktionalität des Gesamtsystems (Energiequelle) für die Teilsysteme hinsichtlich der Grundfunktionen (z. B. Fahren) und Schnittstellenbeschaltung bzw. -konfiguration (mechanisch, elektrisch, hydraulisch, pneumatisch), vergleiche [7].

Zustand „Ist-Status WORK”
- Kommando: v_soll = “don’t care”
- Kommando: Position_HKH = 100%
- Kommando: Übersetzungsstufe_HZW = 1000 1/min
- Kommando: Status_HZW = aus
- Kommando: Status_V3_Spuranreißer = blockiert
- Kommando: Sicherungsventile Spuranreißer = offen

Übergangs-bedingung [Soll-Status = ENGAGE]

Zustand „Einsetzpunkt abwarten”
- Kommando: v_soll = v_max
- Kommando: Spuranreißer absenken
- Berechnung des Abstands der Bearbeitungsgrenze (durch Tastendruck festgelegt) bis zum Arbeitspunkt der Kreiselegge (Eingriff der Messerkreisel)
- Berechnung der verbleibenden Zeit t_{Rest} bis zum Treffpunkt Bearbeitungsgrenze/Arbeitspunkt

Übergangs-bedingung [$t_{Rest} \leq$ Absetzdauer_Egge]

Zustand „Heckkraftheber absenken”
- Kommando: Position_HKH = 0%
- Berechnung: v_soll (abhängig von verbleibender Absetzzeit und verbleibender Wegdifferenz)
- Kommando: v_soll = berechneter Wert
- Messung der Absetzzeit der Kreiselegge

Übergangs-bedingung [Position_HKH < 90%]

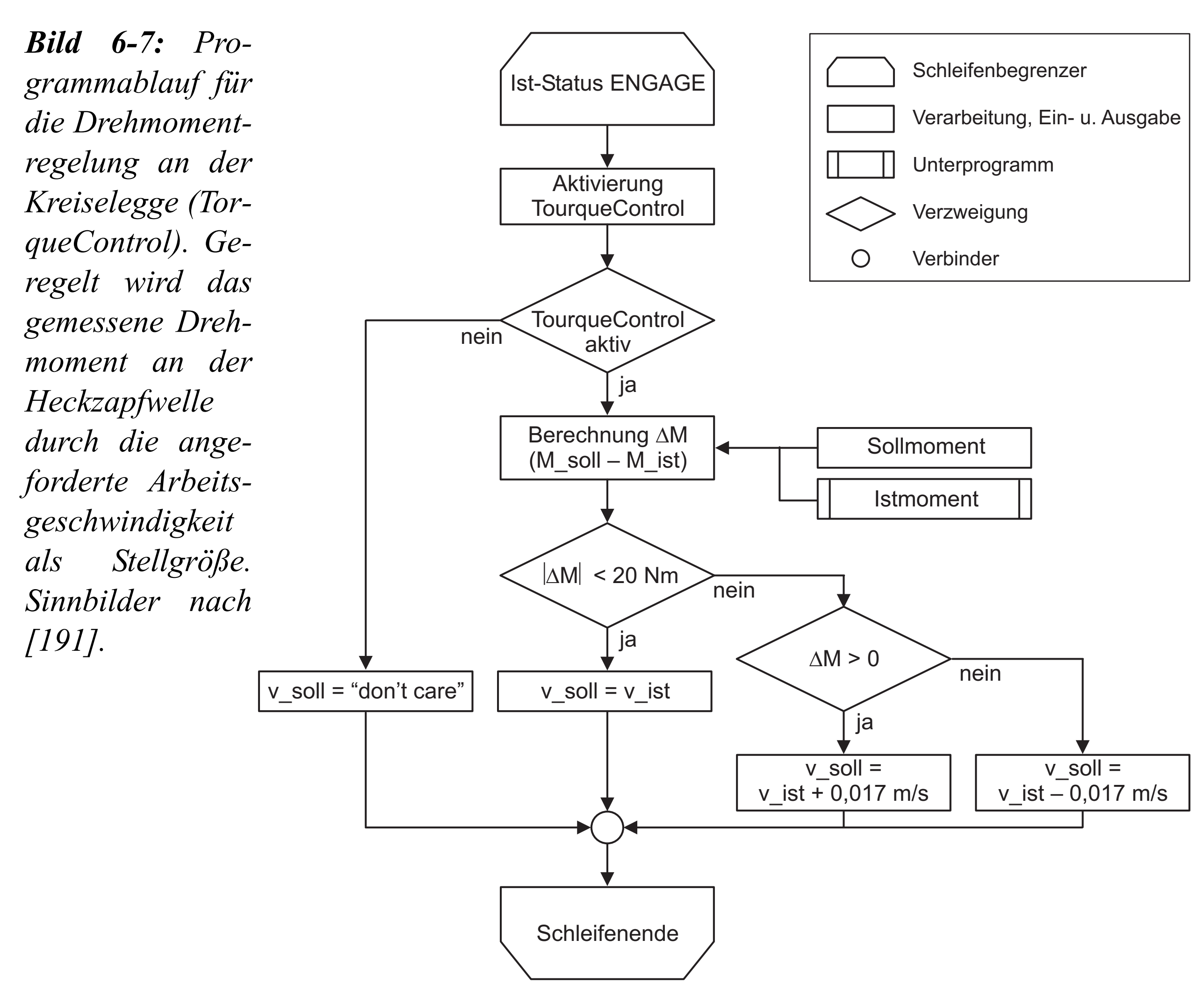
Zustand „Heckzapfwelle einschalten”
- Kommando: Status_HZW = ein
- Berechnung: v_soll
- Kommando: v_soll = berechneter Wert
- Warten bis Ist-Zustand ENGAGE erreicht (u. a. Position_HKH < 40%)
- Messung der Absetzzeit der Kreiselegge und Speicherung für den nächsten Vorgang

Bild 6-6: *Zustandsdiagramm für den Statuswechsel von „Work“ (arbeitsbereit) nach „Engage“ (eingesetzt) der Kreiseleggensteuerung.*

Im Rahmen der Normung zur ISO 11783 wurden verschiedene Arbeitszustände definiert, die für die Geräte bzw. Arbeitsmaschinen zutreffend sind. Neben Zuständen für Transport, Parken und Fehlerstatus sind die Status „Work“ und „Engage“ für die eigentliche Arbeitserledigung der mobilen Arbeitsmaschine vorgesehen. Der Work-Status ist als Übergangs- bzw. Vorbereitungszustand zum eigentlichen Arbeitsprozess definiert – im Anwendungsbeispiel das Positionieren des Gespanns am Vorgewende. Im Zustand „Engage“ erfolgt dann die Erledigung der eigentlichen Arbeit, wie hier das Reihefahren bei der Feldbestellung. Beim gerätegesteuerten Einsetzvorgang vollzieht jedes Gerät am Beginn der Reihe einen Statuswechsel von Work nach Engage, der abhängig von den unterschiedlichen Systemparametern von den Geräten selbst eingeregelt wird – beim Aushubvorgang entsprechend den umgekehrten Wechsel von Engage nach Work. **Bild 6-6** zeigt den Zustandsgraphen mit bedingten Übergängen zwischen den Unterzuständen für den Wechsel der Kreiselegge von Work nach Engage.

Während des Engage-Zustandes bestimmen die Geschwindigkeitslimits der Geräte als festgeschriebene Konfigurationsgröße die Arbeitsgeschwindigkeit des Gespanns. Einzig bei Erreichen des Grenzmomentes an der Zapfwelle sendet die Kreiselegge Geschwindigkeitssollwerte an den Traktor. Die Funktionalität der Momentenregelung während des Reihefahrens ist als Programmablaufplan im **Bild 6-7** gezeigt.

Bild 6-7: *Programmablauf für die Drehmomentregelung an der Kreiselegge (TorqueControl). Geregelt wird das gemessene Drehmoment an der Heckzapfwelle durch die angeforderte Arbeitsgeschwindigkeit als Stellgröße. Sinnbilder nach [191].*



Neben dem sicherheitstechnischen Aspekt der Begrenzung des Drehmoments der Kreiselegge ist es mit der vorgestellten Regelung möglich, durch Vorgabe eines Drehmoments entsprechend der gewünschten Motorauslastung eine Leistungs- bzw. Grenzleistungsregelung an der Zapfwelle zu realisieren [7].

Wendeautomatik am Vorgewende



Bild 6-8: *Versuchsgespann im aufgesattelten und ausgehobenen Zustand beim Wenden am Feldende (Vorgewende). Der Sicherheitsabstand zur Bundesstraße wird überwacht*

Für die sicherheitstechnische Überwachung des Platzbedarfs beim Wenden wurde eine gesonderte Überwachungsfunktion des Traktorrechners implementiert. Um Kollisionen mit Hindernissen oder Einfahren in Gefahrenbereiche, z. B. **Bild 6-8**, zu vermeiden, wird die aktuelle Position, in Verbindung mit den räumlichen Abmaßen und der Orientierung des Gespanns, mit einem vorher vom Fahrer festgelegten rechteckigen Wendebereich abgeglichen. Bei Überlappung des vom Versuchsträger benötigten Raums mit dem Sicherheitsstreifen wird der Fail-Safe-Zustand kontrolliert angefahren.

Grundvoraussetzung für diese MSR-Sicherheitsfunktion ist die Positionsbestimmung des Gespanns relativ zur Bearbeitungsgrenze am Feldende, basierend auf der Erfassung von Lenkwinkel und wahrer Geschwindigkeit, **Bild 6-9** unten. Der Lenkwinkel wird durch einen induktiven Wegaufnehmer und eine Kurvenscheibe mit proportionaler Kennlinie am rechten Vorderrad erfasst und bedarfsweise über die Ackermann-Gleichung [28] auf die linke Fahrzeugseite übertragen. Trotz vorhandenem Radarsensor hat es sich von Vorteil gezeigt, als Geschwindigkeitswert die getriebebasierte Geschwindigkeit der Hinterachse zu verwenden. Der Radarsensor liefert ein zu hohes Rauschen im niedrigen Geschwindigkeitsbereich. Auf Basis des Zweispurmodells [192] wird aus diesen Größen die Bahnkurve des Versuchsträgers, mit Berechnung des Kurswinkels φ und den ortsfesten Koordinaten x_R und y_R des Gespannreferenzpunktes (Mitte Hinterachse), am Vorgewende bestimmt, siehe auch Skizze in Bild 6-9. Durch die geringen Fahrgeschwindigkeiten und das Ausbleiben von Zugkräften beim Wenden können Schräglaufwinkel und Antriebsschlupf mit konstanten Korrekturfaktoren angesetzt und berücksichtigt werden, solange keine starken Steigungen vorliegen.

In einem nächsten Schritt wurde die Positionsbestimmung für die Realisierung einer neuartigen Wendeautomatik weiterverwendet. Nach erfolgter Bearbeitung der Reihe hat der Fahrer die Möglichkeit, die neu realisierte Prozessautomatisierung für das Wenden des Gespanns zu aktivieren. Die Systematik des automatischen Wendevorgangs ist in Bild 6-9 erklärt. Die Automatik erkennt, ob links oder rechts gewendet wird. Bei Aktivierung regelt der Traktorrechner die Geschwindigkeit beim Wenden und invertiert positionsabhängig die Übersetzung. Der Fahrer hat als einzige Aufgabe, das Gespann in drei Wendezügen nach dargestellter Skizze zu lenken. Nach Ablauf des Wendevorgangs startet der Traktorrechner selbstständig die Reihenautomatik für die Bearbeitung der nächsten Bahn punktgenau an der Bearbeitungsgrenze.

Bei den im Kapitel 7.1.1 beschriebenen Versuchsfahrten hat es sich gezeigt, dass die realisierte Positionsüberwachung sicher-

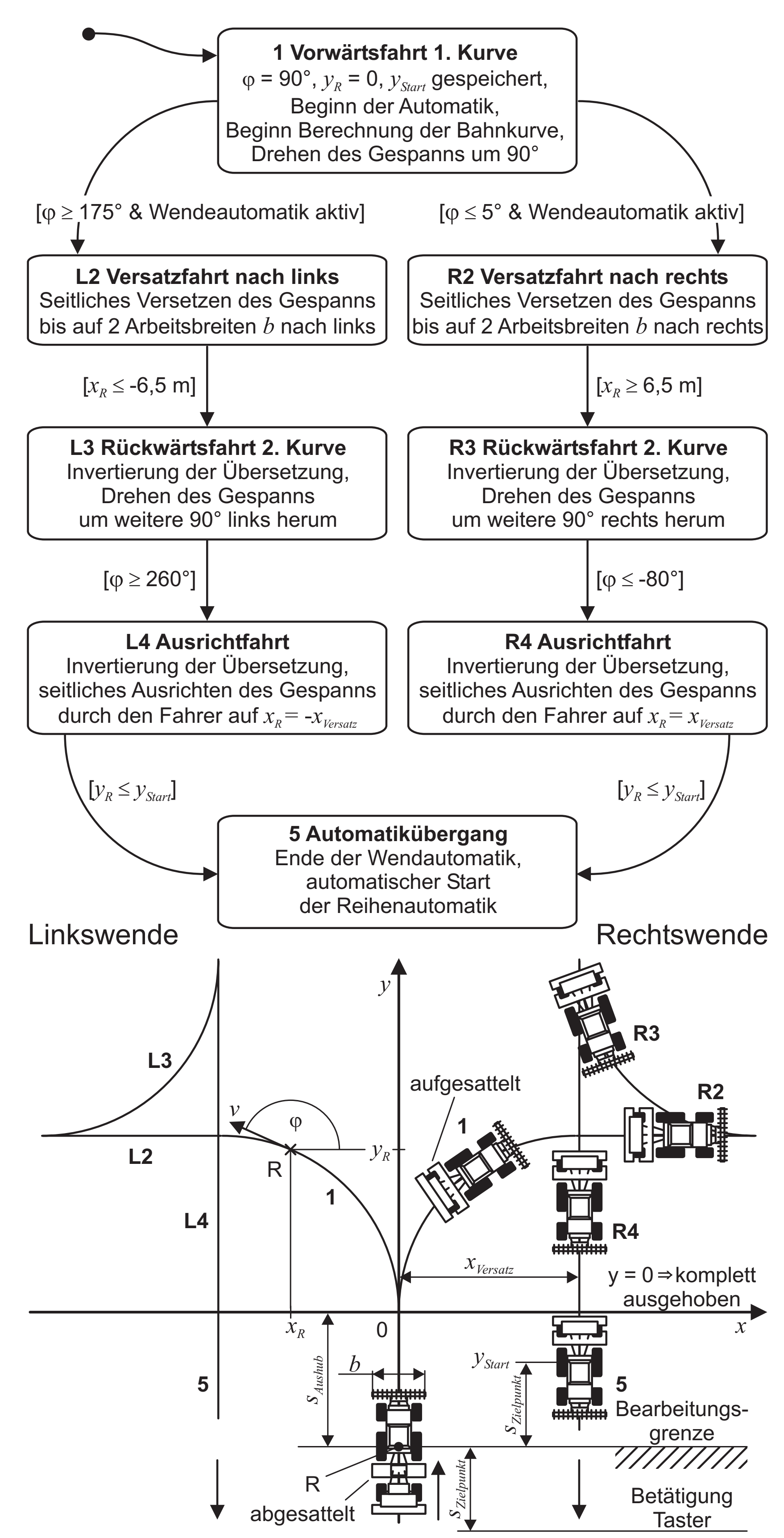


***Bild 6-9:** Zustandsdiagramm und Ablaufdarstellung der Wendeautomatik am Vorgewende. Beim Anschlussfahren gilt $x_{Versatz} = b$.*

heitstechnische Verbesserungen bringt, der teilautomatisierte Wendevorgang aber stark von den äußeren Rahmenbedingungen bei der Feldarbeit abhängt.

6.2 System- und Risikoanalyse der Automatisierungen

Wie in Kapitel 5 gezeigt, sind die parallel wirkenden Methoden Risikoanalyse und System-FMEA die wichtigsten theoretischen Analysemethoden während der Spezifikationsphase des Entwicklungsprozesses. Die Bestimmung des Risikopotenzials und die Lokalisierung potenzieller Fehlerquellen bilden damit die Grundlage der nachfolgenden Entwicklungsschritte. Erster Schritt der Untersuchungen ist die Ermittlung sicherheitsrelevanter Systemzustände aus einem Brainstorming heraus. Die Funktionen des gesamten Maschinensystems stehen dabei im Vordergrund. Die als kritisch eingestuften Zustände werden den betreffenden Teilsystemen zugeordnet und mit Hilfe der Risikoanalyse, siehe Kapitel 4.2.1.2, untersucht. Die komplette Abdeckung aller sicherheitskritischen Teilsysteme lässt ein Profil an geforderten Zuverlässigkeiten entstehen, das sich in den unterschiedlichen Safety-Integrity-Levels (SIL) quantitativ niederschlägt. Die erforderlichen Integritäten der Teilsysteme legen damit die Vorgehensweise im weiteren Entwicklungsprozess fest. Aufbauend auf die Risikoanalyse ermittelt die System-FMEA die potenziellen Fehlerursachen für die herausgefundenen Szenarios (allgemeine Beschreibung der System-FMEA in Kapitel 4.2.1.3). Die Quantifizierung der FMEA-Fehlerfälle mittels Risikoprioritätszahl (RPZ) gibt eine direkte Empfehlung für notwendige, zusätzliche Abhilfemaßnahmen. Umgekehrt ist es im fortschreitenden Entwicklungsprozess sinnvoll, weitere Risikoanalysen dort anzusetzen, wo die FMEA noch unberücksichtigtes Risikopotenzial aufgedeckt hat.

Im Folgenden sollen die für den Versuchsträger durchgeführte Risikoanalyse und die Ergebnisse der System-FMEA am Beispiel automatisierter Eingriffe in den Antriebsstrang vorgestellt werden:

Risikoanalyse für automatisierte Eingriffe in den Antriebsstrang

Die Geschwindigkeitseingriffe durch die beiden implementierten Automatiken wurden im Brainstorming als sicherheitskritisch eingestuft. Bei der Automatik „Gerät steuert Traktor“ senden die landwirtschaftlichen Geräte ihre Sollwerte in Abhängigkeit vom zu erledigenden Prozessschritt, eigener Systemparameter und globaler Umgebungsvariablen über den Geräte-BUS an den Traktorrechner. Der Traktorrechner verarbeitet die gestellten Anforderungen und regelt die ermittelte Zielgeschwindigkeit über Antriebsstrangfunktionen des Traktors ein. Beim automatischen Wendevorgang wird die erforderliche Wendegeschwindigkeit direkt durch den Traktorrechner bestimmt. Der sicherheitskritische Systemzustand liegt in beiden Fällen im unkontrollierten Überfahren der Feldgrenzen durch

die Automatik. Im **Bild 6-10** ist der Risikograph für diesen potenziellen Gefahrenzustand („Hazard“) gezeigt.

Im Bild ist der Pfad für die Ermittlung des Safety-Integrity-Level gezeigt. Das **Schadenausmaß** des Hazards wird mit S2 bewertet. Die in der Regel zu erwartenden Unfälle beim Verlassen des zugewiesenen Arbeitsbereichs des Gespanns sind Kollisionen mit unbeteiligten Personen, ans Feld angrenzenden Hindernissen oder im schwerwiegenderen Fall fahrenden Autos auf der potenziell angrenzenden Bundesstraße. Um die Bewertungskriterien Eintrittswahrscheinlichkeit und Schadenausmaß nicht zu vermischen, sollten keine extremen, unwahrscheinlichen Szenarios herangezogen werden. Recherchiert man die Präventionsberichte der land- und forstwirtschaftlichen Berufsgenossenschaften in Deutschland [193], so machen 99,9% aller registrierten Unfälle mit Todesfolge eine betroffene Person aus. Diese Statistik rechtfertigt eine Einstufung in das Schadenausmaß S2, schwere Verletzung mehrerer Personen bzw. Tod einer Person. Weitere Risikoanalysen zeigten, dass S2 als standardmäßige Bewertung des Schadenausmaßes für die meisten Anwendungsfälle „mobile Arbeitsmaschine beim Arbeitseinsatz“ herangezogen werden kann.

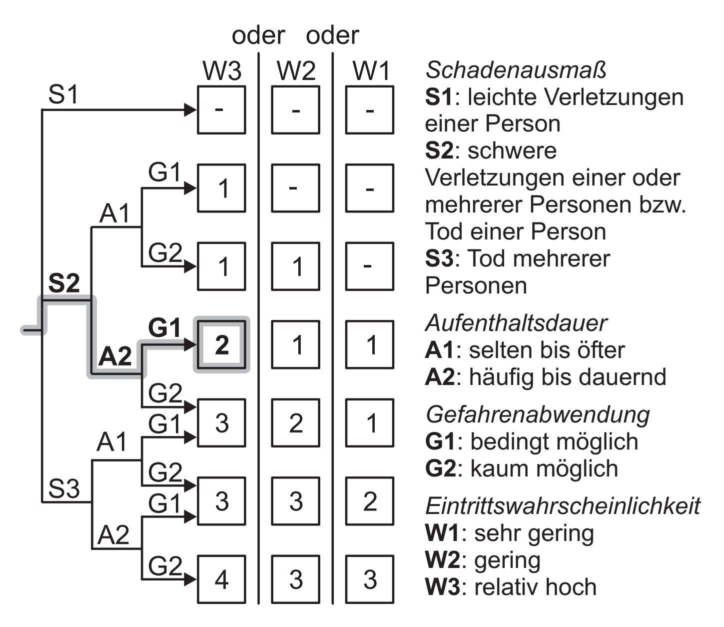


Bild 6-10: *Risikograph für die automatische Geschwindigkeitsregelung des Gespanns zur Ermittlung des entsprechenden SIL (in ☐).*

Die **Aufenthaltsdauer** des Versuchsgespanns im Gefahrenbereich bei zu untersuchendem Szenario, also Bereiche nahe der Feldgrenze (Vorgewende oder Feldrand) wird mit A2 als relativ häufig eingestuft. Diese Situation ist unter Umständen bei jedem Wendevorgang auf den hierzulande kleinen Flächen gegeben.

Die Möglichkeit zur **Gefahrenabwendung** (Bewertung G1) ist für mobile Arbeitsmaschinen da gegeben, wo der Fahrer den Prozess überwacht und innerhalb der Fehlertoleranzzeit die sicherheitskritischen Folgen eines eintretenden Fehlers verhindern kann. Im Anwendungsbeispiel ist der Fahrer oberstes Kontrollorgan und kann den Hazard unter normalen Bedingungen abwenden.

Die **Eintrittswahrscheinlichkeit** des unerwünschten Ereignisses, also in diesem Fall der ungewollte Geschwindigkeitssprung der Traktor/Geräte-Kombination, ist mit W3 als „relativ hoch“ bewertet. Dadurch wird der noch nicht so hohe Reifegrad des innovativen

Systems unter Verwendung moderner Technologien und komplexer Zusammenhänge berücksichtigt. Durch Langzeiterfahrungen und angemessene Entwicklungsprozesse könnte hier die ursprünglich getroffene Bewertung verbessert werden.

Als Ergebnis der durchgeführten Risikoanalyse erhält man eine geforderte Systemintegrität von SIL2, ein typisches Beispiel für ein System mit Fail-Silent-Verhalten. Der sicherheitskritische Fehler muss demnach, auch unter Einbeziehung der Überwachungstätigkeit des Fahrers, erkannt und das System unter Auslösung des Fail-Safe in den sicheren Zustand überführt werden können. Auch die anderen untersuchten Funktionalitäten ergaben maximal eine Einstufung nach SIL2. Da die Automatiken meist durch verteilte Funktionen unter Zusammenspiel mehrerer Logiken realisiert werden, kann man hier nicht zwischen hohen und niederen Integritätsstufen trennen. Sämtliche Steuergeräte und mechatronischen Systeme der Zusatzausrüstung müssen also mit SIL2-gerechten Methoden und Maßnahmen entwickelt werden. Eine nach SIL2 geforderte Entwicklungsmethode ist die nachfolgend beschriebene System-FMEA.

System-FMEA externer, automatisierter Geschwindigkeitsregelungen

In der Risikoanalyse der externen Geschwindigkeitsregelung wurde der Fehlerfall „unkontrolliertes Überfahren der Feldgrenzen“ als sicherheitskritischster Hazard identifiziert und deshalb eingehend in der System-FMEA untersucht. In **Bild 6-11** ist ein Auszug des entsprechenden Formblatts nach VDA 96 [164] gezeigt, in dem die fehlerhafte Ansteuerung der Motordrehzahl behandelt wird. Weitere System-FMEA sind für weitere Fehlerquellen (z. B. Getriebeverstellung) notwendig.

Für den oben genannten sicherheitskritischen Fehler sind mehrere Ursachen, wie z. B. die falsche Priorisierung der Geschwindigkeit durch den Traktorrechner denkbar. Um konkurrierende Kommandos der Geräte auf die Systemgeschwindigkeit aufzulösen, war anfangs die Übergabe von Geschwindigkeitsintervallen als Sollwerte an den Traktorrechner angedacht. Der Traktorrechner sollte durch Schnittmengenbildung entscheiden, welche Geschwindigkeit eingeregelt wird. Da es sich hier um eine innovative Systemauslegung mit wenigen Erfahrungswerten und vielen Fehlermöglichkeiten z. B. in den Bereichen Datenkommunikation und Sensorik handelt, wurde das Auftreten A der Ursache mit acht (erhöht, immer wiederkehrend) unter Berücksichtigung der bestehenden Vermeidungsmaßnahme bewertet. Zusammen mit der Entdeckungsmaßnahme „Fahrerbeobachtung und -eingriff“ (Entdeckenswahrscheinlichkeit E bewertet mit drei, d. h. gut) und der kritischsten Topfehlerfolge „Personenschaden“ (Bedeutung B: äußerst schwerwiegend, d. h. Bewertung zehn) ergab sich eine RPZ von 240. Als notwendige Abhilfemaßnahme wurde die Vereinfachung der Strategie durch Priorisierung der niedrigsten geforderten Geschwindigkeit vorgeschlagen (A: gering, d. h. Bewertung vier). Durch die neue Vermeidungsmaßnahme konnte das Risiko auf eine RPZ von 120 abgesenkt werden.

LTM	**Fehlermöglichkeits- und -einflussanalyse** ☐ *System-FMEA Produkt* ☒ *System-FMEA Prozess*			*FMEA-Nr.:* 0208 *Seite* 3 *von* 6
Typ/Modell/Fertigung/Charge: "Gerät steuert Traktor" Fendt 716/Lemken Gespannkombination		*Sach-Nr.:* 01 *Änderungsstand:* -	*Verantw.:* mm, fr, pi *Firma:* Lehrst. Landmas.	*Abt.:* - *Datum:* 8.5.02
System-Nr./Systemelement: Automat. Ausheben *Funktion/Aufgabe:* Regelung der Geschwindigkeit		*Sach-Nr.:* 01 *Änderungsstand:* 01	*Verantw.:* mm, fr, pi *Firma:* Lehrst. Landmas.	*Abt.:* - *Datum:* 3.6.02

Mögliche Fehlerfolgen	*B*	*Möglicher Fehler*	*Mögliche Fehlerursachen*	*Vermeidungs-maßnahmen*	*A*	*Entdeckungs-maßnahmen*	*E*	*RPZ*	*V/T*
Gespann überfährt Feldgrenze	5	plötzlicher Gasstoß beim Aushub-vorgang	Falsche Gesch-windigkeit wird priorisiert	*Anfangsstand:* 08.05.02					
				Schnittmenge gültiger Geschw.-Intervalle	8	Fahrer-beobachtung und -eingriff	3	240	
Kollision mit Hindernis	7			*Änderungsstand:* 03.06.02					
				niedrigste Geschwindig. gilt	4	s.o.	3	120	
Personen-schaden	10		Ist-Geschwin-digkeit fehler-haft	*Anfangsstand:* 08.05.02					
				Zuverlässige Sensorik	5	Plausibilisierung Geschwindig-keitsmessung Traktor/Gerät	2	100	
			Automatik stoppt nicht	*Anfangsstand:* 08.05.02					
				Lastenheft Programmierung	8	Fahrer-beobachtung und -eingriff	3	240	
				Änderungsstand: 03.06.02					
				Teil-FMEA erforderlich	?	s.o.	3	?	

Bild 6-11: *Auszug aus dem FMEA-Formblatt VDA 96 [164] der System-FMEA „Gerät steuert Traktor“. Bewertungskatalog für B, A und E siehe Anhang 9.1.*

Die potenzielle Fehlerursache „Automatik stoppt nicht“ kann ebenfalls einen plötzlichen Gasstoß am Feldende bewirken. Dieser Fehler ist im Programmablauf der Automatik begründet und daher abhängig vom Lastenheft der Programmierung der Geräterechner oder des Traktorrechners. Da sonst keine weitere Vermeidungsmaßnahme vorgesehen ist, ist auch hier mit einem entsprechend hohen Auftreten zu rechnen (A = 8). Wie im vorigen Beispiel liegt eine mögliche Fehlerentdeckung in der Verantwortung des Fahrers (E = 3) und das Gesamtrisiko ebenfalls im kritischen Bereich (RPZ = 240). Nachdem hier nicht nur ein einzelner Algorithmus als Ursache identifiziert werden kann, sondern die Programmierung und das Zusammenspiel mehrerer Steuerrechner, wird als Abhilfemaßnahme die weitere Untersuchung mittels detaillierter Teil-FMEA vorgeschlagen (siehe Änderungsstand im Formblatt).

Genauso wie die Geschwindigkeitsregelung über Motor und Getriebe wurden auch die anderen Funktionalitäten des Traktorrechners und der drei Geräterechner mit der Methode System-FMEA untersucht. Die lokalisierten sicherheitstechnischen Schwachstellen der Automatisierungen konnten auf diese Weise nachgebessert oder mit zusätzlichen MSR-Sicherheitsfunktionen abgesichert werden.

6.3 Entwicklung ausgewählter MSR-Sicherheitsfunktionen

6.3.1 Entwicklung einer fehlertoleranten Sensorerfassung

Bei der zunehmenden Verbreitung von automatisierten Vorgängen bei mobilen Arbeitsmaschinen werden sich auch Systeme mit hohen sicherheitstechnischen Anforderungen etablieren, wo die reine Fehlererkennung und das darauf folgende sichere Abschalten des Systems (Fail-Silent) als fehlerbeherrschende Maßnahmen nicht mehr genügen. Die geforderte Integrität wird in diesen Fällen mit SIL3 eingestuft und bedingt Fail-Operational arbeitende Systeme, die nach dem Entdecken eines Fehlers ihre Funktion voll aufrechterhalten können, auch wenn Teile des Systems fehlerhaft bzw. gar nicht mehr arbeiten. Beispiele hierfür wären Steer-by-Wire-Systeme bei schnell fahrenden Arbeitsmaschinen im Transporteinsatz oder Systeme mit autonomer, fahrerloser Arbeitserledigung. Die geforderte Fehlertoleranz wird hierbei meistens mit mehrkanalig ausgeführten Architekturen realisiert, siehe Kapitel 5.1.

Auch wenn die Prozessautomatiken des verwendeten Versuchsträgers auf Grund der durchgeführten Risikoanalyse einen Safety-Integrity-Level von maximal SIL2 erfordern, sollen am Beispiel der Aufsattelkinematik der Drillmaschine die Anwendungsmöglichkeiten und Realisierung einer SIL3 genügenden, fehlertoleranten Sensorerfassung gezeigt werden.

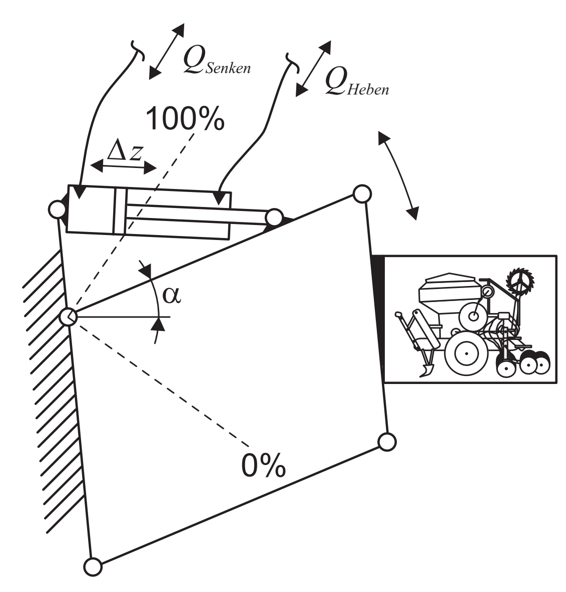


***Bild 6-12:** Systematischer Aufbau der Aufsattelung der Drillmaschine.*

Bild 6-12 zeigt den prinzipiellen Aufbau der Kinematik für die Aufsattelung der Drillmaschine auf die Kreiselegge. Durch Betätigung des entsprechenden hydraulischen Zusatzventils am Traktor wird der doppelt wirkende Zylinder beaufschlagt und die Drillmaschine, im Bild symbolisch dargestellt, über eine parallel geführte Kinematik auf die Kreiselegge aufgesattelt (0% entspricht ganz unten, eingesetzt; 100% ganz oben, ausgehoben). Für die Architektur der fehlertoleranten Erfassung der Aufsattelposition wurde ein 3-kanaliger Aufbau nach Bild 5-5 gewählt. Die ersten beiden Kanäle gewinnt man durch redundant angebrachte Winkelaufnehmer für den Hubwinkel α. Der dritte Kanal wird durch analytische Redundanz aus dem gemessenen Volumenstrom des Zylinders ermittelt. Durch Auswertung des Volumenstroms Q_{Heben} an der Kolbenseite des Zylinders

und Berücksichtigung der kinematischen Größen wird der Ersatzwert $\alpha_{3_analytisch}$ berechnet und mit den beiden gemessenen Winkeln verglichen.

Für die Berechnung des normierten Hubwinkels (Wertebereich von 0 bis 100%) werden die Länge z des Zylinders, ermittelt über Integration von Q_{Heben} bezogen auf die Kolbenringfläche A_{Ring}, Gleichung (6-1), und die geometrischen Winkelbeziehungen der Kinematik (Kosinussatz) herangezogen.

$$\Delta z = -\int \frac{Q_{Heben}}{A_{Ring}}\, dt \qquad (6\text{-}1)$$

Grundlage für die Diagnose eines defekten Winkelsensors bzw. Fehlers in der Kinematik ist die logische Verarbeitung der drei redundanten Kanäle mittels 2oo3-Entscheidung. Dabei werden die Werte durch Berechnung dreier Residuen miteinander verglichen. **Bild 6-13** zeigt den Systemaufbau für die Ermittlung der Messwerte, das analytische Prozessmodell sowie die Bestimmung der Residuen r_1 bis r_3. Die Auswertung obliegt dem Steuerrechner der Drillmaschine.

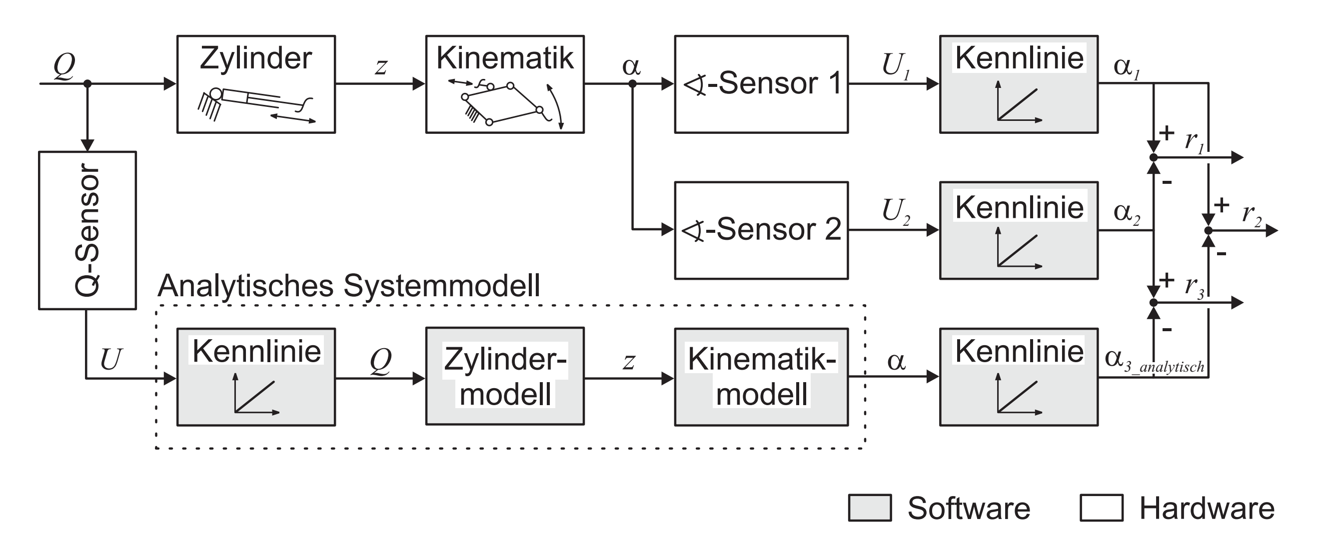


***Bild 6-13:** Signalflussplan der fehlertoleranten Sensorerfassung für die Aufsattelposition der Drillmaschine mit Bestimmung der Residuen durch analytische Redundanz.*

Auf Basis der Entscheidungsmatrix in **Tabelle 6-4** bestimmt der Rechner der Drillmaschine die erforderlichen sicherheitstechnischen Maßnahmen. Beim Abweichen von jeweils zwei Residuen von Null kann der Fehler eindeutig einem bestimmten Sensor bzw. auch der Kinematik der Aufsattelung zugeschrieben werden. Die daraus resultierenden Maßnahmen sind die Rekonfiguration des Referenzwertes auf den verbleibenden, noch funktionierenden Winkelsensor und die Meldung des sicherheitskritischen Fehlers an den Fahrer. Ein Einfachfehler wird somit fehlertolerant abgefangen. Bei systematischen Fehlern liegen meistens keine eindeutig interpretierbaren Diagnoseergebnisse vor und sie sind nicht stochastisch vorhersehbar. Auch in diesem Fall wird auf den nicht betroffenen Wert

umgeschaltet bzw. beim Abweichen aller drei Residuen die aktuelle Quelle (standardmäßig Winkelsensor 1) beibehalten. In jedem Fall wird eine Warnmeldung ausgegeben.

Tabelle 6-4: *Entscheidungsmatrix der drei Residuen für die Fehlerdiagnose. Der Referenzwert $\alpha_{Referenz}$ wird als gültiger Winkel interpretiert und weitergegeben.*

Residuum r_1 $\alpha_1 - \alpha_2$	**Residuum r_2** $\alpha_1 - \alpha_{3_analytisch}$	**Residuum r_3** $\alpha_2 - \alpha_{3_analytisch}$	**Diagnose**	**Referenzwert** $\alpha_{Referenz}$
0	0	0	Kein Fehler	α_1
≠ 0	0	0	Systematischer Fehler	$\alpha_{3_analytisch}$
0	≠ 0	0	Systematischer Fehler	α_2
0	0	≠ 0	Systematischer Fehler	α_1
≠ 0	≠ 0	0	∢-Sensor 1 ϟ	α_2
≠ 0	0	≠ 0	∢-Sensor 2 ϟ	α_1
0	≠ 0	≠ 0	Q-Sensor ϟ, Kinematik ϟ	α_1
≠ 0	≠ 0	≠ 0	ϟ, Systematischer Fehler	α_1

Die Entscheidungslogik und das Vorgehen bei der Rekonfiguration innerhalb der zulässigen Fehlertoleranzzeit wurden in der Model-in-the-Loop-Simulation an der simulierten, hydraulisch betätigten Aufsattelkinematik entwickelt und erprobt. **Bild 6-14** zeigt den Messschrieb einer Simulation. Während des Aushebens wird nach etwa 3,5 s dem Winkelsensor 1 ein Offset-Fehler aufgeschaltet. Da das Toleranzband der Residuen 1 und 2 über-

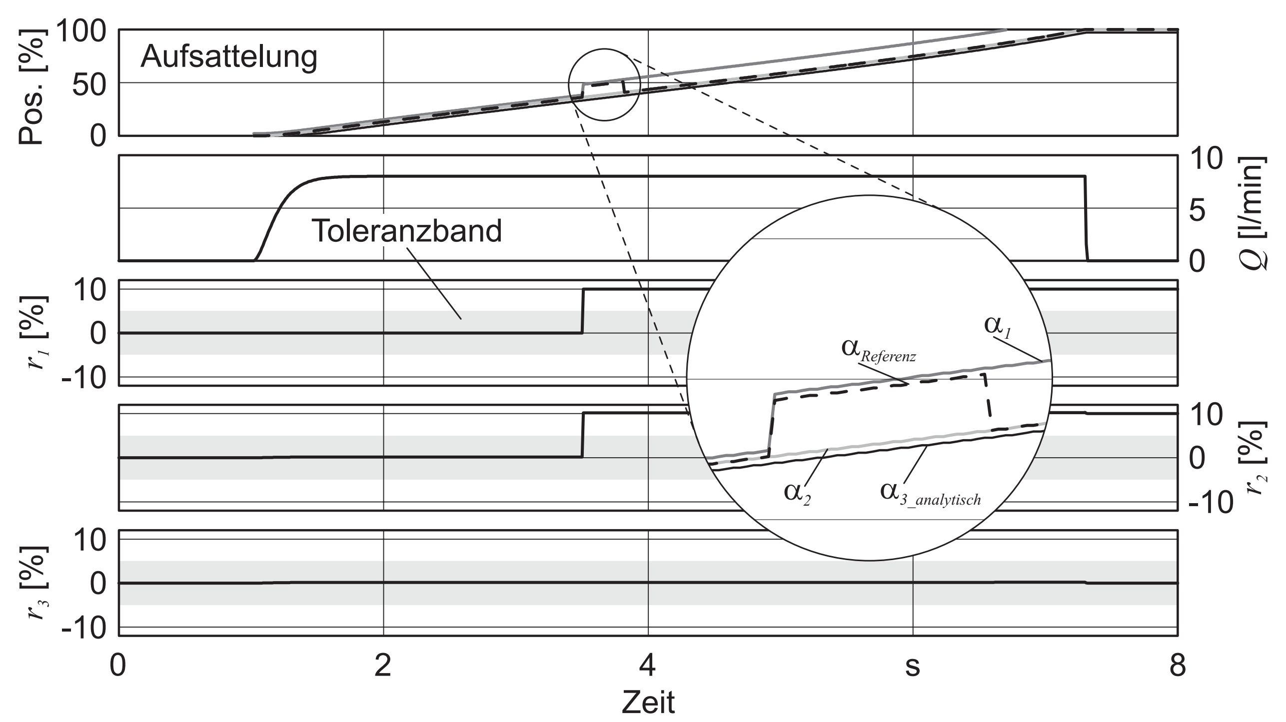


Bild 6-14: *Aufsattelvorgang im MIL-Test der fehlertoleranten Sensorerfassung. Nach Erkennen eines Offset-Fehlers am Winkelsensor 1 (Residuum 1 und 2 ungleich Null) erfolgt die Rekonfiguration auf den redundanten Sensor 2.*

schritten wird, erkennt die Logik den sicherheitskritischen Fehler und wirkt diesem durch Rekonfiguration auf den nicht betroffenen Sensor 2 innerhalb der Fehlertoleranzzeit entgegen. Die Toleranzbänder für die Residuen von jeweils +/- 5% sind nötig, um geringe Abweichungen der Sensoren zueinander bzw. Ungenauigkeiten des Prozessmodells zu berücksichtigen.

Die auf dem Seriensteuergerät implementierte fehlertolerante Sensorerfassung wurde zusätzlich in einem Hardware-in-the-Loop-Test validiert und daraufhin im realen Versuchsgespann in Betrieb genommen, siehe dazu Kapitel 7.1.2.

Da das realisierte System an zusätzliche, relativ aufwendige Sensorik für die genaue Erfassung des Ölstroms gebunden ist, liegt es nahe, nach günstigeren Alternativen der Volumenstrombestimmung zu suchen. Eine Möglichkeit liegt in der Verwertung der Diagnosebotschaften der hydraulischen Zusatzventile bezüglich der Schieberstellung des Ventils in Verbindung mit Messung des Druckunterschieds zwischen Pumpendruck und Lastdruck auf der Heben-Seite des Zylinders. Aufgrund der Load-Sensing-Hydraulik des Traktors kann durch diese Größen mit relativ geringem sensorisch Aufwand auf den tatsächlichen Ölfluss in oder aus dem Zylinder geschlossen werden, siehe auch nachfolgend Gleichung (6-2). Grundvoraussetzung für diese Vorgehensweise ist die Bestimmung einer genauen Kennlinie für den Öffnungsquerschnitts des Ventils in Abhängigkeit von der Schieberstellung.

6.3.2 Entwicklung einer sicherheitsgerechten Ressourcenverteilung für den hydraulischen Durchfluss

Die System- und Risikoanalyse der Funktionalität „Gerät steuert Traktor“ hat gezeigt, dass automatische Zugriffe auf die Traktorarbeitshydraulik (Zusatzventile, Hubwerke) verschärfte Anforderungen an die Ressourcenverteilung stellen. Die Situation hydraulischer Unterversorgung tritt bei manueller Betätigung alleine durch den Fahrer eher selten auf, ist bei zeitgleichem Zugriff der Geräte aber ein häufig vorkommendes Problem. Um die entwickelten Maßnahmen für eine „soziale“ Verteilung des verfügbaren Ölstroms darzulegen, muss zuvor auf das bestehende Hydrauliksystem des Traktors eingegangen werden:

Bei der Arbeitshydraulik vieler mobiler Arbeitsmaschinen ist heute eine Kombination aus Differenzdruckregelung (Load Sensing) und Maximaldruckregelung (aktive Druckabschneidung) üblich, Einzelheiten siehe in [80]. Auch der Versuchstraktor Fendt Favorit 716 ist standardmäßig mit Load-Sensing-Hydraulik ausgerüstet. Die **Differenzdruckregelung** hält den Druckabfall Δp an einem Ventil durch automatische Pumpenverstellung konstant und regelt so den Volumenstrom Q. Modelliert man die Strömung durch das Proportionalventil als Blendenströmung nach Gleichung (6-2) wird das Regelprinzip deutlich:

$$Q = \alpha \cdot A \sqrt{\frac{2 \cdot \Delta p}{\rho}} \tag{6-2}$$

Unter der Annahme eines nahezu konstanten Durchflusskoeffizienten α und gleich bleibender Dichte ρ hängt der Volumenstrom bei konstant geregeltem Druckunterschied Δp direkt vom Öffnungsquerschnitt A der Blende, bzw. des Ventils ab.

Bild 6-15 beschreibt das Prinzip der Differenzdruckregelung für die gleichzeitige Beschaltung mehrerer Verbraucher. Auf die übliche Maximaldruckregelung wurde in der Darstellung aus Platzgründen verzichtet. Aufbau und Funktionsweise sind für mehr als zwei Verbraucher analog.

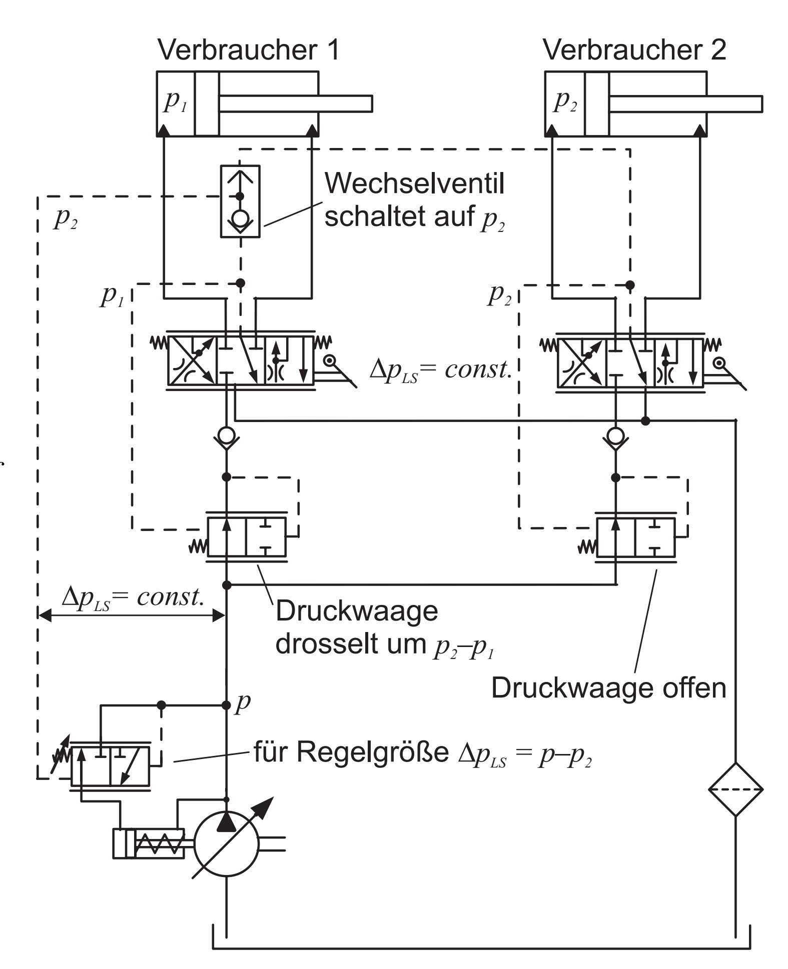


Bild 6-15: *Hydraulisch-mechanische Differenzdruckregelung (Load Sensing) nach [80]. Gezeigt ist der Anwendungsfall bei gleichzeitiger Betätigung der 5/3-Wegeventile unter der Lastannahme $p_2 > p_1$. Die Verstellpumpe regelt den Druckabfall am lastdruckhöheren Proportionalventil unabhängig von Ventilstellung, Pumpendrehzahl und Druckniveau auf den konstanten Differenzwert Δp_{LS}. Das Wechselventil meldet dabei der Pumpe den jeweils höchsten Lastdruck zurück. Die Druckwaage des geringer belasteten Verbrauchers 1 erzeugt die benötigte Druckdifferenz Δp_{LS} an diesem Proportionalventil bei gleichzeitiger Drosselung um den Betrag $p_2 - p_1$.*

Reicht der verfügbare Gesamtvolumenstrom der Pumpe aus, können alle Verbraucher ohne gegenseitige Beeinflussung versorgt werden. Probleme treten auf, wenn der geforderte Gesamtvolumenstrom der Ventile den maximalen Förderstrom der Pumpe überschreitet. Die konventionelle Differenzregelung gerät in Unterversorgung. Der Verbraucher mit dem höchsten Lastdruck verlangsamt seine Bewegung unter Umständen bis zum Stillstand.

Differenzdruckregelung mit nachgeschalteten Druckwaagen – LUDV[1)]

Um möglichen Funktionsstörungen bei Unterversorgung von Verbrauchern herkömmlicher LS-Systeme zu begegnen, wurden Differenzdruckregelungen mit nachgeschalteten Druckwaagen entwickelt, die nach dem Stromteilerprinzip arbeiten und eine den geforderten Volumenströmen äquivalente Aufteilung – auch bei Unterversorgung – gewährleisten [194, 195]. **Bild 6-16** erklärt das Prinzip dieser „sozialen" Durchflussverteilung.

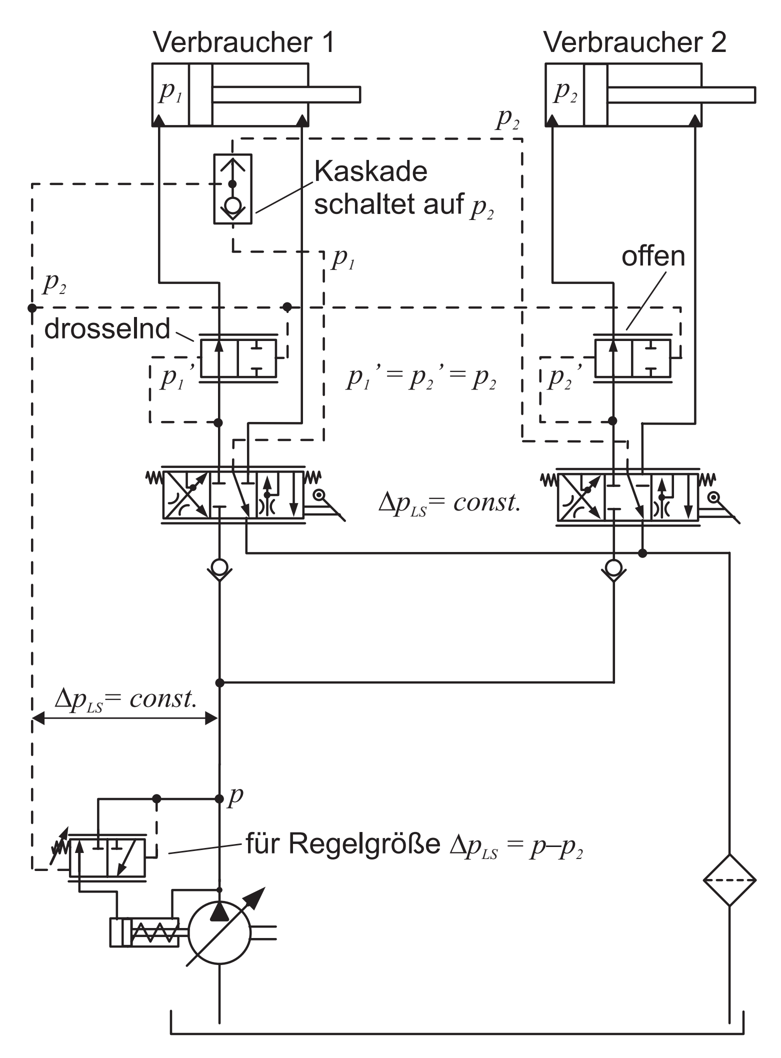


***Bild 6-16:** Differenzdruckregelung mit nachgeschalteten Druckwaagen für eine gerechte Durchflussverteilung bei Unterversorgung (LUDV). Anwendungsbedingungen: Es gilt $p_2 > p_1$ und beide Verbraucher sind zu versorgen. Die Druckwaagen werden vom höchsten Lastdruck p_2 vorgesteuert und bilden diesen hinter den 5/3-Wegeventilen ab. Durch das Gleichgewicht $p_1' = p_2' = p_2$ bleibt auch das Druckgefälle Δp_{LS} (Regelgröße der Verstellpumpe) konstant. Bei Unterversorgung sinkt der Druck vor den Wegeventilen und damit der Druckabfall Δp_{LS} gleichmäßig. Die Volumenströme reduzieren sich dadurch im Verhältnis der Öffnungsquerschnitte der Proportionalventile: $Q_1/Q_2 = A_1/A_2$, entsprechend Gleichung (6-2).*

Die rein hydraulisch-mechanisch realisierte, soziale Durchflussverteilung ist ein fehlersicheres System, das auch bei hydraulischer Unterversorgung den sicherheitskritischen Stillstand des höchst belasteten Verbrauchers verhindern kann. Hauptanwendungsbereich derartiger Differenzdruckregelungen mit nachgeschalteten Druckwaagen sind Baumaschinen, bei denen die Koordination mehrerer hydraulischer Funktionen auch sicherheitstechnisch schon lange notwendig ist. Es ist sicherlich möglich, das vorgestellte Prinzip auch in anderen Sparten mobiler Arbeitsmaschinen einzusetzen. Die Wirtschaftlichkeit und

1) Mittlerweile etabliert sich die Bezeichnung „Lastdruckunabhängige Durchflussverteilung" (LUDV), geprägt durch die Fa. Bosch Rexroth.

sicherheitstechnische Notwendigkeit über das Anwendungsbeispiel hinaus waren aber nicht Gegenstand der Untersuchungen.

Elektronisch geregelte Durchflussverteilung

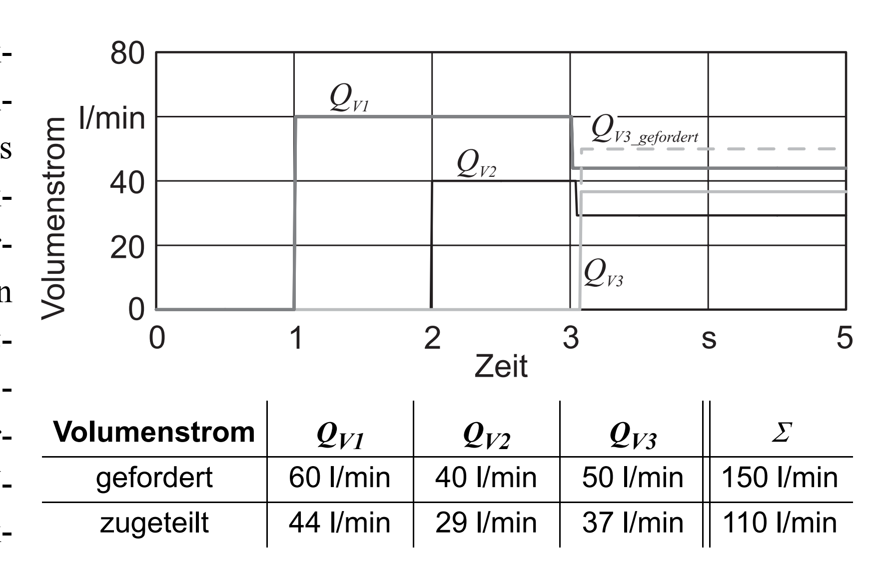
Ein weiteres Konzept zur Realisierung der „sozialen“ oder auch „gerechten“ Ressourcenverteilung des hydraulischen Volumenstroms ist die elektronische Begrenzung des geforderten Gesamtvolumenstroms bei drohender Unterversorgung und zwar unter Beibehaltung des Aufbaus der konventionellen Load Sensing Arbeitshydraulik. Für das Versuchsgespann wurden zwei unterschiedlich wirkende Konzepte entwickelt und in Betrieb genommen:

Untergeordnete Priorisierung durch den Geräterechner: Liegen mehrere hydraulische Verbraucher im Aufgabenbereich eines landwirtschaftlichen Gerätes, z. B. der Aufsattelzylinder und der Gebläse-Ölmotor der Drillmaschine, kann das Gerät selbstständig entscheiden, welche Funktion die sicherheitstechnisch wichtigere ist. Wird ein Geschwindigkeitsverlust oder der Stillstand dieser Funktion erkannt, ändert das Gerät seine Befehle an den Traktor und schaltet auf Notbetrieb. Der unwichtige Verbraucher, hier der Gebläseantrieb, wird abgeschaltet, um das korrekte Ausheben der Drillmaschine sicherzustellen. Voraussetzung für diese Vorgehensweise ist das Vorhandensein sicherheitstechnisch verzichtbarer Funktionen mit ausreichendem Volumenstrombedarf, der bei zurückgewonnener Verfügbarkeit den Volumenstrommangel beseitigen kann.

Übergeordnete Verteilung durch den Traktorrechner: Ein weiterer universeller Ansatz ist die Überwachung und eventuelle Anpassung aller geforderten Volumenströme durch einen übergeordneten Kontrollrechner. Im Anwendungsbeispiel wurde diese MSR-Sicherheitsfunktion dem Traktorrechner zugeteilt. Er überwacht den Status und die geforderten Volumenströme für die hydraulischen Zusatzventile und die Kraftheber und vergleicht den gesamten Volumenstrombedarf $Q_{gefordert}$ mit dem zur Verfügung stehenden Wert $Q_{verfügbar}$. Wird der verfügbare Ölstrom von dem geforderten überschritten, werden die Volumenströme der Konfigurationsbefehle für die beaufschlagten Zusatzventile nach Gleichung (6-3) reduziert, eine Unterversorgung wird verhindert.

$$Q_{neu} = Q_{alt} \cdot \frac{Q_{verfügbar}}{Q_{gefordert}} \qquad (6\text{-}3)$$

Bild 6-17 zeigt die Wirkungsweise der elektronisch gesteuerten, sozialen Durchflussverteilung als Messschrieb einer MIL-Simulation für die Verifikation der verwendeten Logik. In zugehöriger Tabelle sind die geforderten und durch die Überwachung angepassten Volumenstromwerte für das Beispiel aufgeführt.



Volumenstrom	Q_{V1}	Q_{V2}	Q_{V3}	Σ
gefordert	60 l/min	40 l/min	50 l/min	150 l/min
zugeteilt	44 l/min	29 l/min	37 l/min	110 l/min

Bild 6-17: *MIL-Simulation der elektronisch geregelten Durchflussverteilung bei Unterversorgung. Bei 3 Sekunden wird* $Q_{verfügbar}$ *(110 l/min) überschritten. Die Volumenstromanforderungen werden daraufhin automatisch mit dem Faktor* $Q_{verfügbar}/Q_{gefordert}$ *= 110/150 reduziert.*

Zur Realisierung der elektronisch geregelten Durchflussverteilung musste das Elektronikkonzept des Traktors verändert werden. Im ursprünglichen System wurden die hydraulischen Zusatzventile und der Frontkraftheber über den Fendt-Fahrzeugrechner mittels CAN-Botschaften auf dem Traktor-BUS II angesprochen. Der vorhandene Softwarestand des Versuchstraktors erlaubte es nicht, die Durchflussmengen mehrerer Ventile in **einem** Vorgang zu verändern. Dies konnte nur durch ein direktes Ansprechen der Ventile (Fa. Bosch) realisiert werden, weshalb der Traktor-BUS II aufgebrochen wurde und die Zusatzventile zusammen mit dem Frontkraftheber separiert wurden, **Bild 6-18**. Die Durchflussbefehle gelangen daraufhin vom Traktorrechner (MicroAutoBox) über den Traktor-BUS I zum Mess-Laptop. Dieses verarbeitet die Befehle über eine CAN-Programmierung (CANalyzer) und schickt sie über Bosch-Telegramme auf den Ventil-BUS. Da der Fendt-Fahrzeugrechner die Diagnoseantworten der Bosch-Ventile plausibilisiert, mussten diese über einen zusätzlichen Steuerrechner (im Bild gestreift dargestellt) auf dem Traktor-BUS II emuliert, d. h. durch Software nachgebildet werden.

Bei dieser Umsetzung konnten nicht alle Verbraucher der Arbeitshydraulik berücksichtigt werden. Im verwendeten Versuchstraktor sind die Volumenströme der Kraftheber vorne und hinten aus systematischen Gründen nicht online konfigurierbar. Die eingeprägten Durchflüsse der Hubwerke wurden jedoch, genauso wie die von der Motordrehzahl abhängige Volumenstromgesamtmenge, bei der Bestimmung von $Q_{verfügbar}$ berücksichtigt.

Um die Vorteile beider elektronischer Konzepte zu vereinen, wäre eine elektronisch realisierte, soziale Durchflussverteilung sinnvoll, die mit einer zusätzlichen Priorisierungsmöglichkeit des sicherheitsrelevantesten Verbrauchers erweitert werden kann. Auch bei hohen Überschreitungen des verfügbaren Volumenstroms wäre so die Verfügbarkeit der Sicherheitsfunktion sichergestellt. Beide Konzepte wurden im Vergleich zur her-

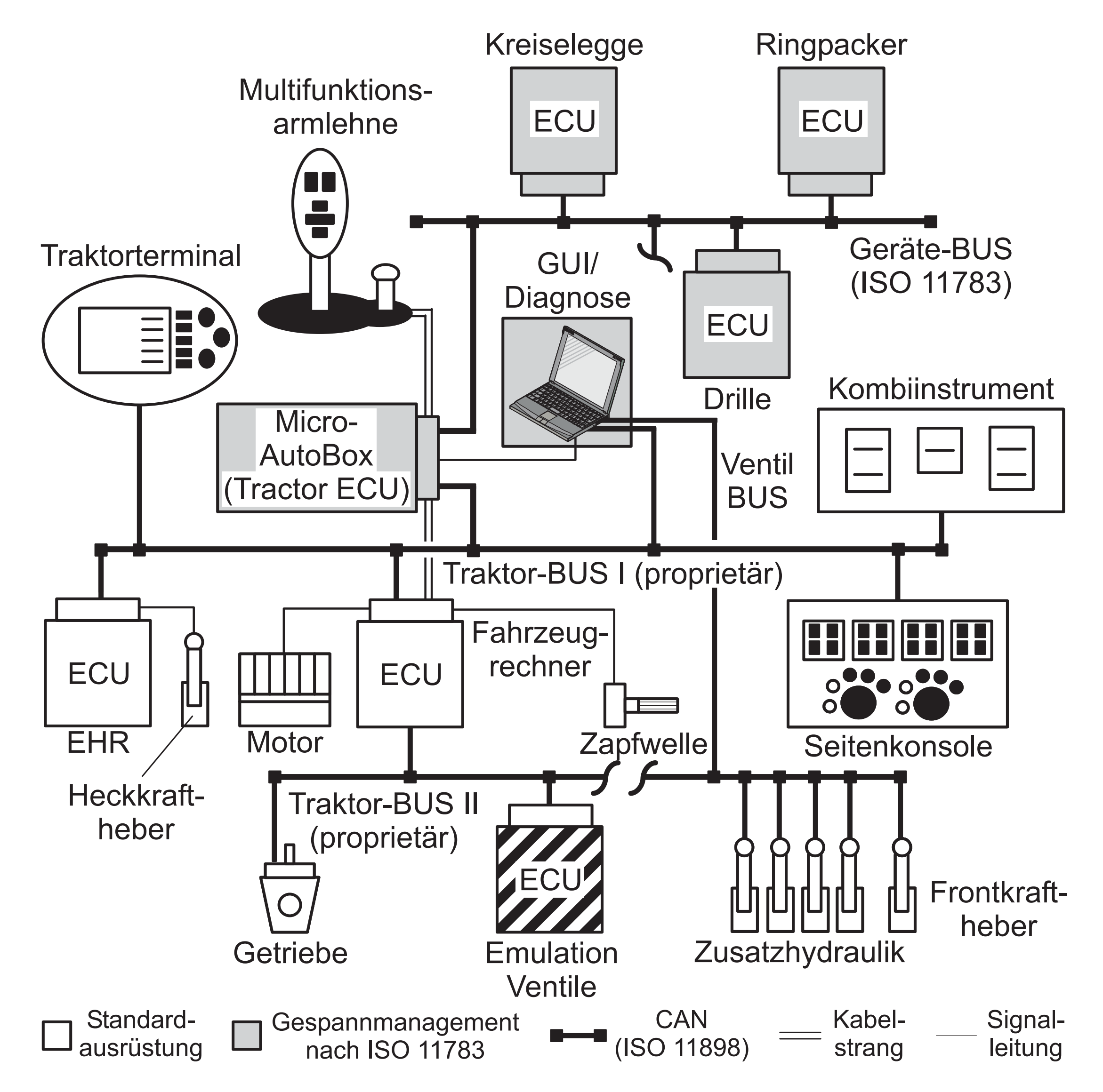


Bild 6-18: *Die erweiterte Elektronikarchitektur ermöglicht das direkte Ansprechen der Ventile für die Realisierung der elektronisch geregelten sozialen Durchflussverteilung.*

kömmlichen Hydraulik in Versuchsfahrten untersucht und validiert, siehe Kapitel 7.1.3. Die erreichten Ergebnisse unterstreichen die sicherheitstechnische Notwendigkeit der Vermeidung der Unterversorgung einzelner Verbraucher.

6.3.3 Modellbasierte Entwicklung des Traktorrechners – Geschwindigkeitsregelung

In den aufgeführten Ausschnitten der System- und Risikoanalyse für die automatische Geschwindigkeitsregelung durch den Traktorrechner wurden die sicherheitstechnischen Anforderungen an die Automatisierungen deutlich. Am Beispiel der Entwicklung des Traktorrechners soll die Anwendung einer modellbasierten Vorgehensweise für sicherheitsrelevante Systeme gezeigt werden.

Hauptfunktionalität der Geschwindigkeitsregelung ist die Umsetzung der ermittelten Sollgeschwindigkeit in Stellbefehle an den Fahrzeugrechner des Traktors. Mit Hilfe von Eingriffen in den Antriebsstrang bezüglich Motordrehzahl, Vorwärts/Rückwärts-Schaltung, Beschleunigungsstufen I bis IV[1)] und der Einstellung der Übersetzung über die vom Traktorrechner simulierte Fahrhebelauslenkung wird die Sollgeschwindigkeit des Systems am Versuchsgespann eingeregelt. Die entsprechenden Signale werden von der MicroAutoBox mit diskreten Ausgängen für den Fahrzeugrechner so generiert, dass diese sich nicht von denjenigen der normalen Betätigung der Elemente der Armlehne unterscheiden, vergleiche Systemaufbau in Bild 6-2. Je nach Anwendungsfall ergibt sich die Sollgeschwindigkeit aus geräteseitigen Anforderungen, Vorgaben der Wendeautomatik, sicherheitstechnischen Maßnahmen oder durch Fahrereingaben.

Das Verhalten der grafisch programmierten Geschwindigkeitsregelung konnte in einem ersten Schritt in der **Model-in-the-Loop-Simulation** des Traktors modular entwickelt werden. Der Traktor wurde mit seinem Antriebsstrang und den notwendigen Trägheiten mathematisch logisch mit Matlab/Simulink abgebildet. Abhängig vom Unterschied von Soll- und Istwert der Geschwindigkeit schaltet die MicroAutoBox die Beschleunigungsstufen und regelt über Fahrhebelkommandos die Soll-Geschwindigkeit ein, **Bild 6-19**. Die Intervalle der Soll/Ist-Abweichungen für die jeweilige Beschaltung der Stufen I bis IV waren für Schnelligkeit und Stabilität der Regelung ausschlaggebend und wurden in der MIL-Simulation optimiert. Die so entwickelten Reglermodelle konnten in der graphischen Programmierung (Abbildung mit Matlab/Simulink und der Zustandmaschine Stateflow) des Traktorrechners eins zu eins übernommen werden.

Im folgenden **HIL-Test** des Traktorrechners wurde die MicroAutoBox über die HIL-Umgebung DS1103 der Fa. dSPACE in die Echtzeitsimulation des Traktors eingebunden. Die für die Geschwindigkeitsregelung relevanten Ein- und Ausgänge wurden nach außen geführt und mit den realen Messwerten des Versuchsfahrzeugs abgeglichen. Mit der HIL-Untersuchung war es möglich, den gesamten Steuerrechner, mit Programmierung und Peripherie, auf seine Spezifikation hin zu testen.

Nach der Integration der MicroAutoBox in den Traktor wurde die Regelung mittels **Rapid-Control-Prototyping** ans reale Fahrzeug angepasst, um noch bestehende Fehler der Programmierung zu beseitigen. Der Vorteil der verwendeten MicroAutoBox als RCP-Hardware zeigte sich bei der Parametrisierung der entwickelten Algorithmen. Durch den Online-Zugriff auf sämtliche Parameter der Regelung in Echtzeit und der Möglichkeit zur

1) Der Favorit 716 bietet vier wählbare Beschleunigungsstufen, die sich in der Geschwindigkeitsänderung beim einmaligen Antippen bzw. im Gradienten beim stetigem Auslenken des Fahrhebels unterscheiden.

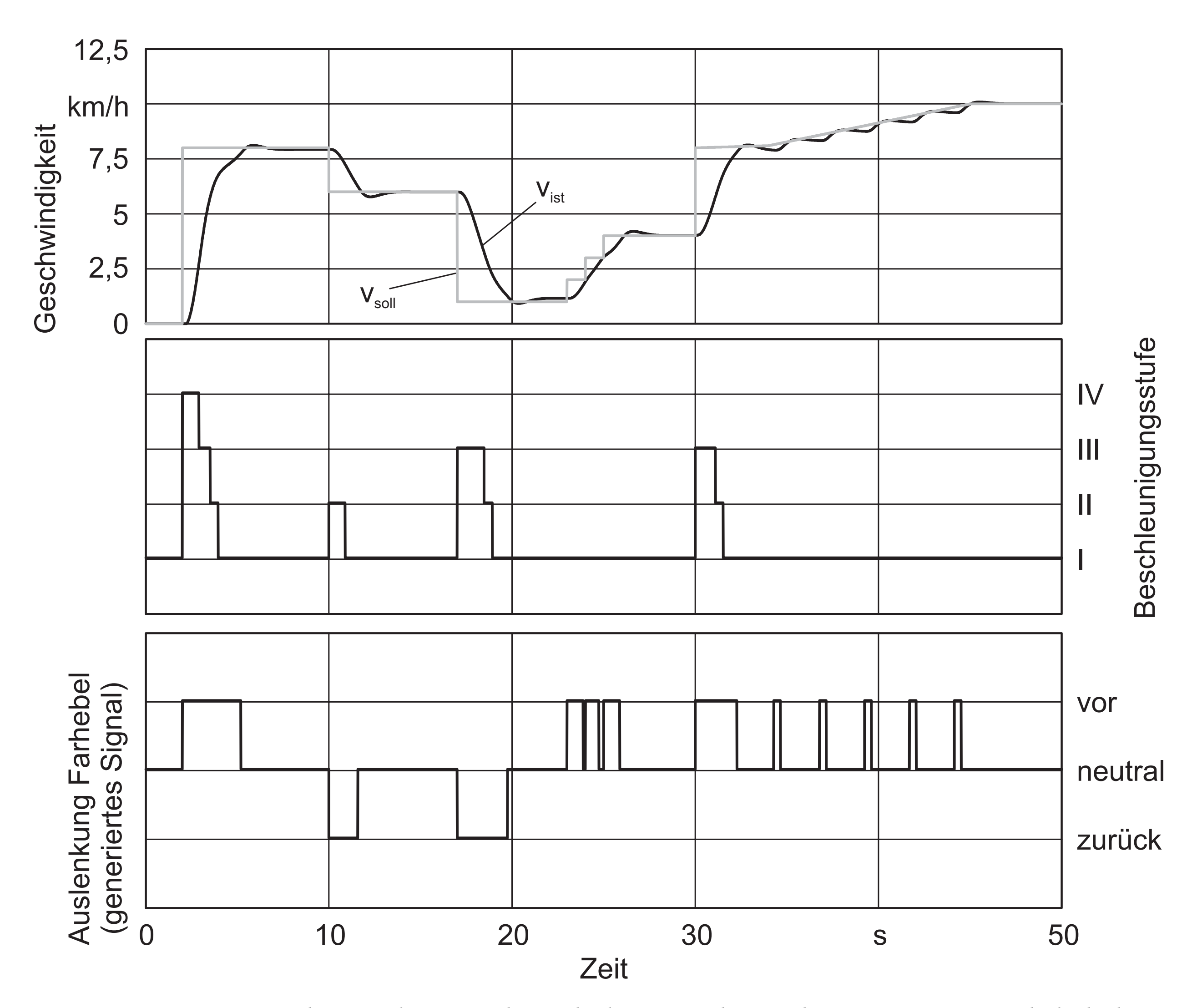


Bild 6-19: *MIL-Simulation der Geschwindigkeitsregelung über generierte Fahrhebelsignale und automatisiertes Schalten der Beschleunigungsstufe.*

Veränderung der Werte, konnten die Regler adaptiv im realen Fahrzeug und unter realen Einsatzbedingungen optimiert werden.

6.3.4 Modellbasierte Entwicklung des Rechners der Kreiselegge – automatische Generierung von Serien-Code

Bei der Entwicklung des Steuerrechners der Kreiselegge sollten Machbarkeit und Vorteile einer **durchgängig** modellbasierten Entwicklung der Steuergerätesoftware gezeigt werden. Wie zuvor in Kapitel 4.3.5 beschrieben, können die gesamten Pluspunkte nur durch Verwendung eines automatischen Serien-Code-Generators genutzt werden, der die kontinuierliche Bearbeitung der Programmlogik von der Spezifikation bis zur Codierung in **einer** Entwicklungs-Umgebung ermöglicht. Der Stand der Technik automatischer Code-Generatoren beschränkt sich größtenteils auf die Generierung einzelner Funktionsmodule, die daraufhin händisch in das Serien-Code-Projekt eingepflegt werden. Ziel war es, den

Code-Generator TargetLink (Fa. dSPACE) für die Codierung des kompletten Softwareprojekts der Kreiselegge zu verwenden. Die Schwierigkeit lag dabei in der Nutzung steuergerätespezifischer Funktionen (Ein-/Ausgänge und sonstige BIOS-Funktionen), die durch spezielle Usercode-Blöcke implementiert werden mussten.

Um eine universelle Plattform – auch für die Entwicklung anderer Logiken gleicher Hardwarebasis – zu erhalten, wurde ein auf das Steuergerät ESX 2 angepasstes Matlab/Simulink-Rahmenmodell entwickelt, in das beliebige Funktionsmodelle eingesetzt werden können, **Bild 6-20**. Das Rahmenmodell beinhaltet dabei die Schnittstelle zu den benötigten BIOS-Funktionen der ESX. Neben Modellierung des Steuergeräte-Codes im Funktionsmodell wurden die Regelstrecken für die Systemparameter der Kreiselegge in das Gesamtmodell mit aufgenommen, um die Untersuchung der Logik in der MIL-Simulation zu ermöglichen. Aus dem eingebetteten Funktionsmodell kann über TargetLink der komplette Serien-Code für die Zielhardware generiert werden.

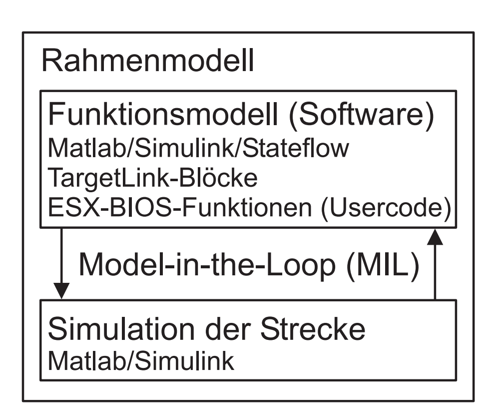


Bild 6-20: *Rahmenmodell zur Generierung der ESX-Steuergerätesoftware. Zur Verifikation wurde die Simulation der Regelstrecke integriert (MIL-Tests).*

Die in **Bild 6-21** gezeigte Vorgehensweise bei der modellbasierten Entwicklung des Geräterechners mit automatischer Code-Generierung ist wie folgt: Schon in der Spezifikationsphase werden die Einzelfunktionen in Matlab/Simulink/Stateflow umgesetzt und an der Abbildung der Strecke Model-in-the-Loop getestet. Zur späteren Code-Generierung müssen die normalen Simulink-Blöcke durch parametrisierbare TargetLink-Blöcke im Funktionsmodell ersetzt werden. Sind die Ein- und Ausgänge sowie die erforderlichen Sende- und Empfangstelegramme der CAN-Kommunikation festgelegt, müssen diese Objekte aus der speziell entwickelten ESX-Blockbibliothek kopiert werden. Zusätzlich initialisiert man diese einmalig in den Usercode-Modulen *TL_main.** und *CAN_Egge.**, womit das Rahmenmodell an die Ein-/Ausgabestruktur des Steuergerätes vollständig angepasst ist. Das eingebettete Softwaremodell wird mit der Modellierung der Strecke zum Gesamtmodell (*ESX.mdl*) erweitert. Aus diesem Modell heraus kann einerseits die Programmlogik erneut mit MIL getestet, andererseits der Serien-Code über TargetLink unter Zugriff auf den verknüpften Usercode generiert werden. Das aus der Programmlogik entstehende Softwareprojekt wird direkt im standardmäßig verwendeten Compiler zu einer auf den Flash-Speicher des Steuergeräts übertragbaren Datei (*ESX.hex*) weiterverarbeitet. Während der gesamten Testdurchführung (MIL-Test, HIL-Test oder realer Versuch) können die erkannten Softwarefehler direkt im Funktionsmodell beseitigt werden – der

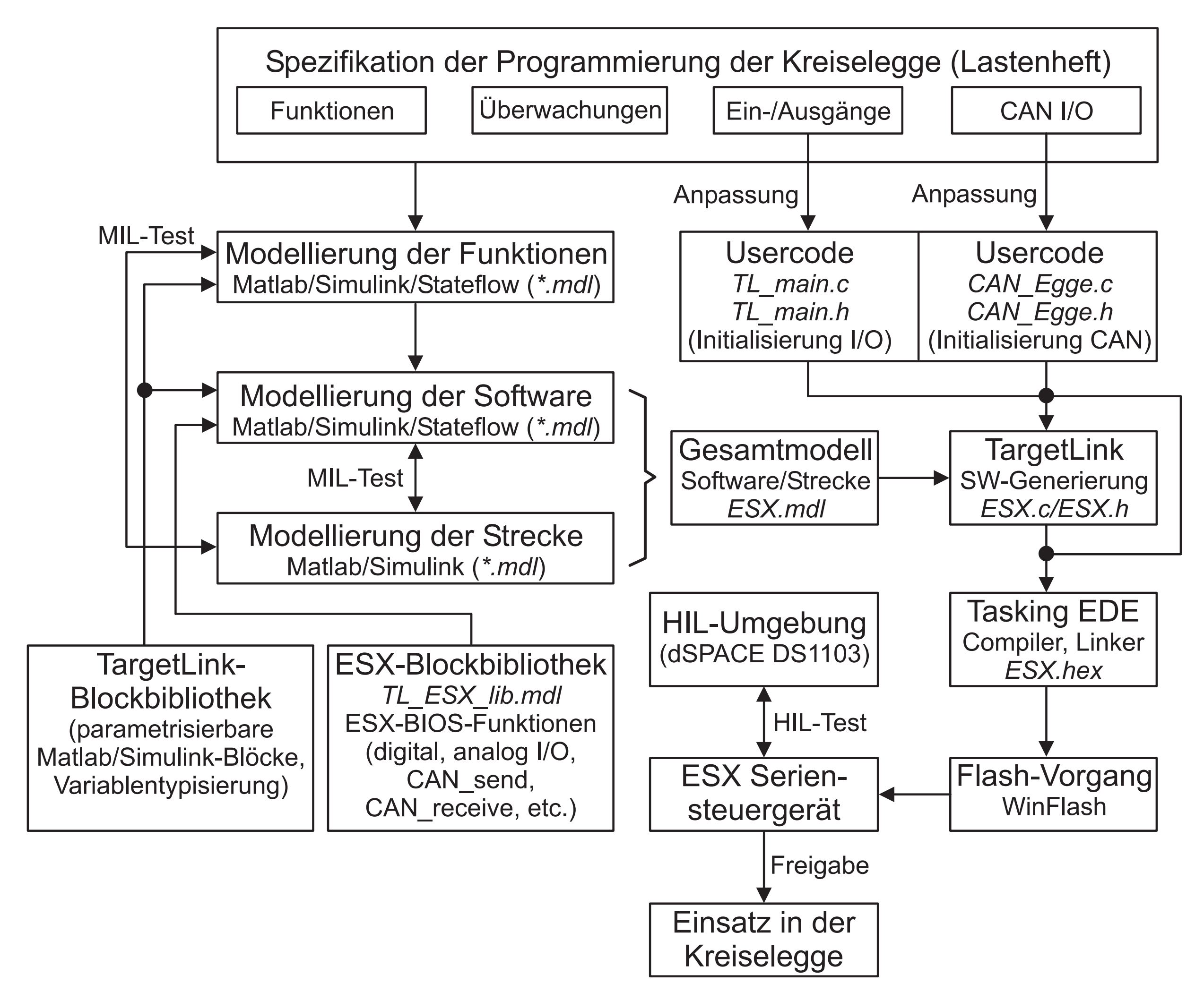


Bild 6-21: *Vorgehen bei der automatischen Generierung von Serien-Code für die Kreiselegge. Das Einbinden von Usercode-Blöcken ermöglicht die Verwendung von an die ESX angepassten, steuergerätespezifischen BIOS-Funktionen bei der Softwaremodellierung. Diese Funktionen sind in der entwickelten ESX-Blockbibliothek zusammengefasst.*

Serien-Code muss so nicht händisch, wie im Vorgehen ohne automatischen Code-Generator, an den Änderungsstand der Modelle angepasst werden.

Um die Vorteile und Nachteile der automatischen Generierung von Serien-Code gegenüber konventioneller, manueller Codierung abzuwägen, wurde der Steuerrechner der Kreiselegge unter beiden Vorgehensweisen zweigleisig entwickelt. Die so parallel codierten Softwareprojekte wurden auf die korrekte Erfüllung der gemeinsamen Spezifikation hin getestet. Sowohl in der MIL-Simulation, im Hardware-in-the-Loop-Test als auch im realen Feldversuch konnten keine signifikanten Unterschiede zwischen händisch erstelltem und aus der graphischen Programmierung automatisch generiertem Serien-Code festgestellt werden. Im Gegenteil, durch die verbesserte Übersichtlichkeit der graphischen Darstellung konnten Umsetzungsfehler erkannt werden, die in der konventionell programmierten Steuerung nicht auffielen.

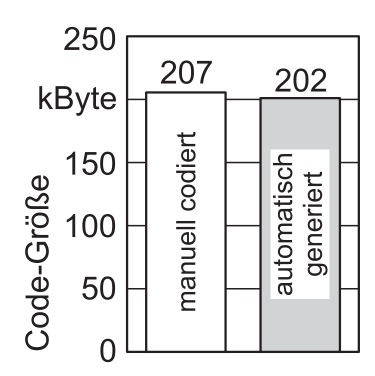


***Bild 6-22:** Code-Effizienz anhand des Größenvergleichs der kompilierten Hex-Files.*

Ein oftmals erwähnter Nachteil automatischer Code-Generatoren ist die relativ schlechte Code-Effizienz. Ein Maß dafür ist das Verhältnis der Größe des kompilierten Codes zum erreichten Funktionsumfang. Je effizienter Lastenheft und Programmierung umgesetzt wurden, desto kleiner ist das entstehende Hex-File und desto besser sind i. a. Laufzeitverhalten und Speicherbedarf. Im Anwendungsbeispiel wurden beide Vorgehensweisen verglichen, **Bild 6-22**. Die Dateigrößen lagen dabei auf sehr ähnlichem Niveau. Durch geschickte Programmierung auf der einen oder anderen Seite lässt sich die Code-Effizienz stark beeinflussen. Gut programmierter händischer Code schneidet jedoch im breiten Anwendungsfeld generell besser ab als automatisch generierter. Die Problematik der Code-Effizienz wird sich jedoch mit Ausreifen der Generatoren und steigenden Hardwareleistungen weiter verringern. Zusammenfassend zeigt folgende Aufstellung die Aspekte, die mit einer, auf automatischer Code-Generierung aufbauender, modellbasierten Entwicklungskette verbunden sind:

- Schaffung von gut lesbarem, dokumentiertem Serien-Code
- Vermeidung von Programmier- und Umsetzungsfehlern
- frühe Testbarkeit der Funktionen
- Vereinfachung des Änderungsmanagements
- höhere Transparenz der Programmlogiken
- Erleichterung der Wiederverwendbarkeit der Module (Abstraktion der Hardware)
- Verkürzung der Entwicklungszeit
- automatische Berücksichtigung von Softwarestandards

aber

- hoher Initialaufwand bei Anpassung des Erstellungsprozesses an Serienhardware
- Code-Effizienz zurzeit noch schlechter als bei manueller Codierung

Die sicherheitstechnischen Vorteile der Vorgehensweise konnten bei der Entwicklung des Kreiseleggenrechners erarbeitet und nachgewiesen werden. Im Zusammenhang mit der Zuverlässigkeit der Werkzeuge hört man oft den Ruf nach zertifizierten Lösungen für Code-Generator und Compiler. Bei durchgeführten Untersuchungen wurde die Verifikation anhand geforderter Spezifikation und korrekter Umsetzung der Programmierung durch den Code-Generator auf Basis konventioneller Testmaßnahmen vollzogen. Zertifizierte Werkzeuge würden jedoch den Testaufwand nur teilweise bis gar nicht verringern. Das korrekte Arbeiten der nicht zertifizierten Tools wird demnach mit dem Funktionsnachweis der fertig programmierten Steuerung „proven in use“ begründet.

7 Versuchsdurchführung und Verallgemeinerung der Ergebnisse

Die entwickelten MSR-Sicherheitsfunktionen wurden zuerst in Simulationen getestet und später sukzessive am realen Versuchsgespann in Betrieb genommen. Wo es möglich war, wurde versucht, die sicherheitstechnischen Überwachungen in statischen Standversuchen oder Fahrversuchen ohne Geräte zu verifizieren. Die eigentliche Validierung wurde mit der gesamten Traktor/Geräte-Kombination in zahlreichen Versuchsfahrten auf dem institutseigenen Versuchsfeld durchgeführt. Die Vorgehensweise gliederte sich anhand der verschiedenen Überwachungsstrategien funktionaler Sicherheit in folgende Bereiche:

- Überwachung sicherheitsrelevanter Prozessgrößen
- Koordination von Bewegungsabläufen
- sicherheitsgerechtes Verhalten der Teilsysteme im Fehlerfall
- korrekte Interpretation und Verarbeitung des Fahrereingriffs

Dieses Kapitel beschreibt die wichtigsten Beispiele für Überwachungsstrategien der Gespannkombination anhand des Versuchskonzepts und verallgemeinert die Ergebnisse auf die Anwendung bei mobilen Arbeitsmaschinen.

7.1 Überwachung sicherheitsrelevanter Prozessgrößen

Der größte Teil der MSR-Sicherheitsfunktionen gilt der Kontrolle gültiger Wertebereiche von sicherheitskritisch eingestuften Prozessgrößen, wobei die Signale real gemessen oder analytisch hergeleitet werden. Ein weiterer Aspekt sind Überwachungen konkurrierender Zugriffe auf gemeinsam verfügbare Systemressourcen, speziell für Systeme mit mehreren gleichberechtigten Geräten.

7.1.1 Überwachung gültiger Bereiche sicherheitsrelevanter Prozessparameter

Klassische Beispiele für Überwachungen gültiger Wertebereiche sind Begrenzungen der Arbeitsgeschwindigkeiten bei landwirtschaftlichen Bodenbearbeitungsgeräten, um Qualitätseinbrüche der Arbeitserledigung zu vermeiden. Im Anwendungsbeispiel sind die Maximalgeschwindigkeiten von Ringpacker, Kreiselegge und Drillmaschine geräteseitig limitiert und werden an den Traktorrechner als Geschwindigkeitslimit des jeweiligen Geräts übergeben. Die Geschwindigkeitssollwerte der Geräte werden somit zweifach mit den festgelegten Grenzwerten abgeglichen, einmal durch Vergleich im jeweiligen Geräterechner und zusätzlich durch Berücksichtigung des kleinsten Limits durch den Traktorrechner. Zusätzlich hat der Fahrer die Möglichkeit, die Arbeitsgeschwindigkeit durch ein über den Taskcontroller eingegebenes Limit pauschal zu begrenzen. Im **Bild 7-1** ist die Geschwindigkeitsbegrenzung durch ein Taskcontroller-Limit v_{max_Task} auf 5,04 km/h gezeigt.

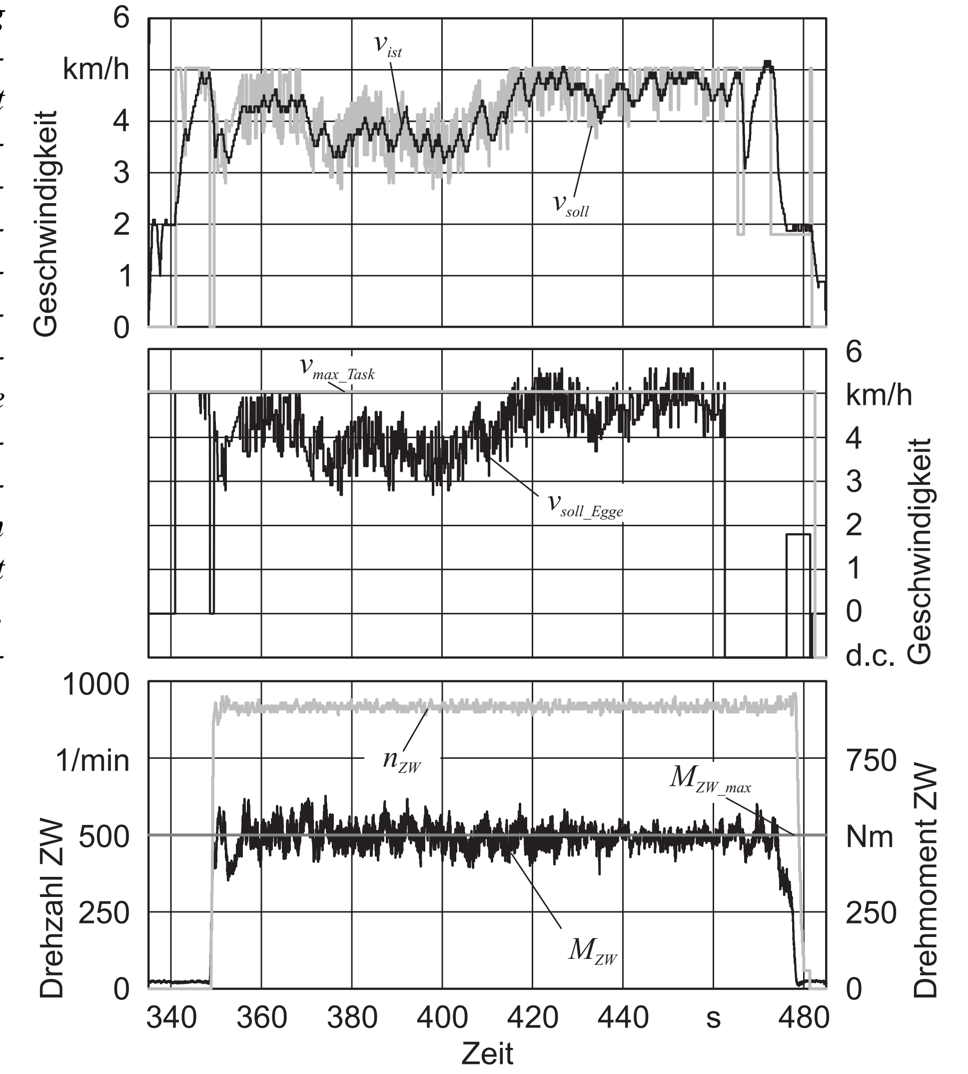


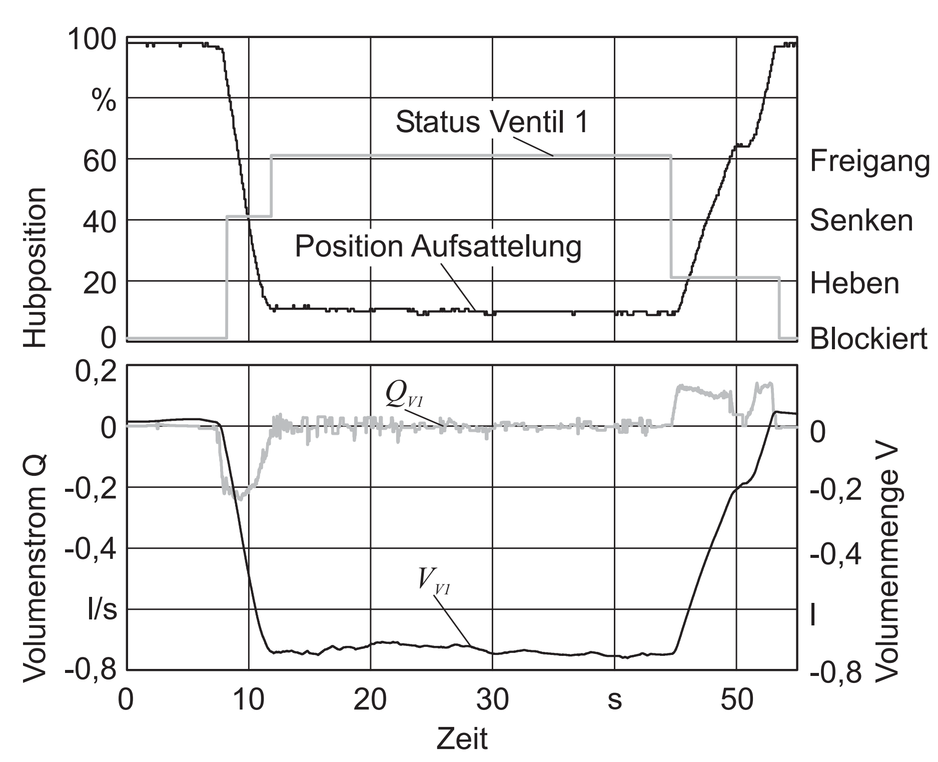
Bild 7-1: *Limitierung der maximal zulässigen Geschwindigkeit durch den Taskcontroller und Begrenzung des Drehmoments an der Zapfwelle durch Anpassung der Soll-Geschwindigkeit über die Kreiselegge. Dargestellt ist eine Reihenfahrt mit Einsetzen und Ausheben („don't care", abgekürzt d. c., bedeutet: keine Anforderung).*

Der mittlere Messschrieb zeigt das Limit des Taskcontrollers sowie die Soll-Geschwindigkeit des Geräterechners der Kreiselegge. Oben befindet sich die durch den Traktorrechner priorisierte Soll-Geschwindigkeit v_{soll} und die eingeregelte Ist-Geschwindigkeit v_{ist}.

Im unteren Teilbild ist als weiteres Beispiel die Überwachung des maximal zulässigen Drehmoments an der Zapfwelle gezeigt. Eine Überlastung des Antriebs der Kreiselegge und vor allem der in den Boden eingreifenden Messerzinken kann dadurch vermieden werden. Aus dem Vergleich des gemessenen Moments M_{ZW} mit der eingestellten Führungsgröße M_{ZW_max} gibt die Kreiselegge ihre Soll-Geschwindigkeit v_{soll_Egge} als Stellgröße an den Traktorrechner. Der relativ geringe Drehmomentgrenzwert von 500 Nm wurde gewählt, um den Einfluss auf die gültige Soll-Geschwindigkeit v_{soll_Egge} deutlich zu machen, da eine höhere Schwelle bei den gegebenen Bodenbedingungen normal nicht erreicht wurde.

Viele kinematische Funktionen bei mobilen Arbeitsmaschinen werden hydraulisch bewerkstelligt. Die Bilanzierung des hydraulischen Ölstroms durch Integration von Hin- und Rückfluss an der Schnittstelle eines Verbrauchers und Ermittlung des abgegebenen Ölvolumens kann Leckagen oder andere sicherheitskritische Funktionsfehler ersichtlich machen. **Bild 7-2** zeigt die Überprüfung des in den Zylinder gegebenen Stoffstroms für die Hubwerkskinematik der Kreiselegge. Nach erfolgtem Absenken und Wiederausheben der Aufsattelung, d. h. Aus- und Einfahren des Zylinders, muss das aufintegrierte Ölvolumen in einem zulässigen Toleranzfeld um Null zu liegen kommen. Ist die Abweichung zu hoch, wird die Sicherheitsfunktion ausgelöst, in diesem Fall der Stopp der Automatik mit Warnmeldung an den Fahrer.

Bild 7-2: *Bilanzierung des hydraulischen Ölstroms am Ventil 1 (Aufsattelung). Dargestellt ist der gemessene Volumenstrom am Schnellkuppler, das aufintegrierte Ölvolumen (Messschrieb unten) sowie die Schaltstellung des Ventils und die resultierende Hubposition der Aufsattelung (Messschrieb oben).*



Viele sicherheitskritische Situationen im Arbeitseinsatz mobiler Arbeitsmaschinen entstehen durch das dynamisch veränderliche Arbeitsumfeld und die dadurch bedingte potenzielle Gefährdung von unbeteiligten Personen. Kann man den Arbeitsbereich vorher räumlich eingrenzen, besteht die Möglichkeit, die Position des Maschinensystems zu überwachen und ein Verlassen des zugewiesenen Arbeitsbereichs durch Sicherheitswarnungen und Noteingriffe zu verhindern. Beispiel hierfür ist der Wendevorgang des Versuchsgespanns auf Schlägen mit angrenzenden sicherheitskritischen Orten, wie hoch frequentierte Feldwege oder Kraftfahrstraßen, wie es in Bild 6-8 ersichtlich wurde. Die dazu implementierte Vorgewendeüberwachung integriert die tatsächliche Geschwindigkeit in x- und y-Richtung des ortsfesten Koordinatensystems am Feldende und ermittelt so die Ist-Position des Gespanns, relativ zum zugewiesenen Wendebereich. Die Ermittlung der relativen Position ist im Messschrieb für zwei Wendemanöver gezeigt (**Bild 7-3**). Ein- und Ausfahrtsrichtung sind auf Grund des pauschal geschätzten Längs- und Querschlupfs (konstante Korrekturfaktoren) nicht ganz parallel.

Die Überwachung der Position erfolgt durch den Traktorrechner und wird nach dem erfolgten Ausheben der Geräte am Feldende ($y = 0$) gestartet. Mit diesem Zeitpunkt wird der Ursprung des Koordinatensystems festgelegt, das System befindet sich im Modus „Wenden“. Im Bild ist die Bahn des Referenzpunktes (Mitte Hinterachse des Traktors) dargestellt. Zusätzlich zur Relativposition des Referenzpunktes wird die Gierrate, gewonnen aus Fahrgeschwindigkeit, Lenkwinkel und Momentanpollage, berechnet. Die Integration der Gierrate ergibt den Kurswinkel des Gespanns relativ zum xy-Koordinatensystem und damit die zu überwachende geometrische Ausdehnung in y-Richtung. Wird die vorher zugewiesene Grenze für den zulässigen Platz am Vorgewende von beispielsweise 15 m überschritten, wird der Fahrer gewarnt und der sichere Zustand eingeleitet.

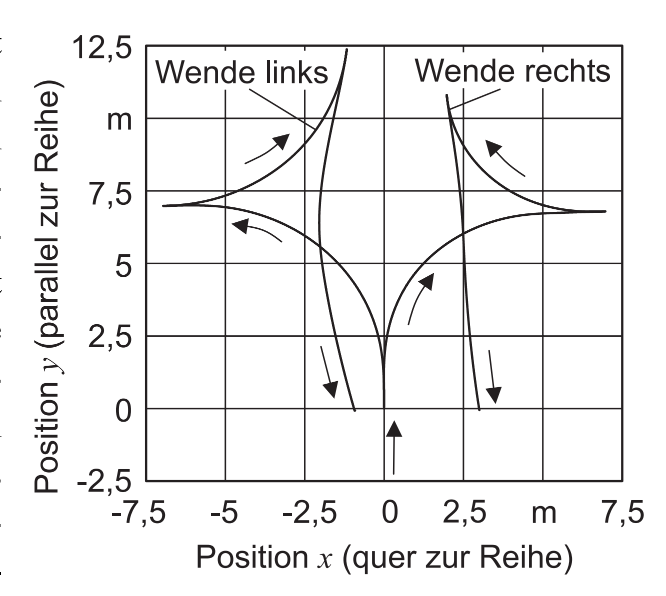


Bild 7-3: *Positionsüberwachung relativ zum Vorgewende. Die y-Koordinate wird mit der maximal zulässigen Ausdehnung verglichen. Dargestellt sind zwei aufeinander folgende Wendevorgänge.*

Auf Basis der Positionsbestimmung am Vorgewende wurde eine Wendeautomatik entwickelt, die dem Fahrer die Regelung von Motordrehzahl, Wendeschaltung, Übersetzungseinstellung und erneutem Start der Reihenautomatik abnimmt, wie ausführlicher im Kapitel 6.1.3 behandelt. Bei den Versuchsfahrten hat es sich gezeigt, dass die Positionsbe-

stimmung allein basierend auf Lenkwinkel und Geschwindigkeit und die damit verbundene Schräglaufwinkel- und Schlupfkompensation im großen Maße von verschiedenen Randbedingungen abhängen. Je nach Feuchte, Bearbeitungszustand, Pflanzenbestand, Geländeprofil, Verschmutzungsgrad des Gespanns und Befüllungszustand des Saatkastens ergeben sich andere Faktoren für die Berücksichtigung des Schräglaufwinkels und des Antriebsschlupfes. Als Ergebnis kann festgehalten werden, dass die entwickelte Wendeautomatik nur mit zusätzlichen Koppelebenen zur Positionsbestimmung, wie GPS-Technik oder Beschleunigungsaufnehmer, eine hohe Präzision des Wiedereinsetzens mit lateralen Fehlern im cm-Bereich gewährleisten kann. Für die sicherheitstechnische Raumüberwachung des Vorgewendes kann diese Lösung jedoch mit einfachen Mitteln eine Vermeidung kritischer Zustände bewerkstelligen, wenn ein genügend großer zusätzlicher Sicherheitsstreifen von z. B. 1 m (normale Bedingungen ohne Gefälle) definiert wird.

7.1.2 Plausibilisierung sicherheitsrelevanter Parameter

Für die indirekte Bestimmung bzw. Abschätzung (Plausibilisierung) sicherheitsrelevanter Parameter kann es im Gegensatz zur direkten sensorischen Erfassung folgende Gründe geben:

- Das zu überwachende Signal ist nur mit großem Aufwand zu erfassen, z. B. bei schwer zugänglichen Messstellen, teuerer Sensorik oder schmutzanfälligen, schwer zu schützenden Einbaustellen.
- Das zu überwachende Signal ist aus anderen schon erfassten Signalen modellbasiert herleitbar, wodurch der Aufwand deutlich vermindert wird. Meistens sind viele Prozessgrößen über digitale Kommunikationssysteme für verschiedene elektronische Steuergeräte ohne großen Aufwand verfügbar, die in direktem Zusammenhang mit anderen gesuchten Größen stehen.
- Das zu überwachende Signal soll fehlertolerant erfasst werden, d. h. es soll zusätzlich zur konventionellen Erfassung mit Hilfe eines oder mehrerer weiterer Kanäle durch analytische Redundanz bestimmt werden (z. B. 2oo3-Architektur). Ein Vergleicher kann aus den unterschiedlichen Signalquellen die fehlerhafte diagnostizieren und das richtige Signal Fail-Operational bereitstellen, siehe Kapitel 5.1.

Hinsichtlich der Genauigkeit des indirekt bestimmten Signals gibt es je nach Anwendungsfall unterschiedliche Ansprüche. Auch mit Prozessdaten grober Auflösung können einzelne Systemzustände oder Größen abgeschätzt werden, wie die beiden folgenden Beispiele zeigen:

1. Über die grob aufgelöste Drehzahl der Packerringe werden zwar relativ ungenaue Geschwindigkeitswerte des Versuchsgespanns ermittelt, ein zu hoher Schlupf der Antriebsräder bzw. ein Stopfen des Ringpackers kann aber trotzdem diagnostiziert werden.
2. Die logische Verarbeitung der Drücke der hydraulischen Zusatzventile bietet die Möglichkeit, die Freigangstellung zu diagnostizieren und den gemeldeten Status plausibilisieren zu können.

Für Zwecke analytischer Redundanz müssen hingegen relativ genaue Messwerte herangezogen und mit einem möglichst der Realität entsprechenden Modell der Strecke verknüpft werden. Wie im Kapitel 6.3.1 beschrieben, wurde am Versuchsträger ein Bespiel für eine fehlertolerante Sensorerfassung mit zwei gemessenen und einem analytisch gewonnen Signal für die Position der Drillenaufsattelung implementiert. Die Risikoanalyse der Prozessautomatik hatte zwar gezeigt, dass eine fehlertolerante Messwerterfassung, wie sie hier realisiert wurde, für den vorliegenden Anwendungsfall normalerweise nicht notwendig ist. Aus Demonstrationsgründen sollte aber ein Fail-Operational-System realisiert werden, wofür die Positionsbestimmung der Aufsattelung ein gutes Beispiel bot, **Bild 7-4**. Der Drehwinkel der Hubwerkskinematik wird durch zwei Hubwinkel, α_1 und α_2, redundant erfasst. Zusätzlich wird durch Integration des Volumenstroms das Ölvolumen in den Hubzylinder der Aufsattelung errechnet und daraus ein dritter Hubwinkel $\alpha_{3_analytisch}$ hergeleitet. Die drei Hubwinkel werden im elektronischen Steuerrechner der Drille ausgewertet und zueinander plausibilisiert. Im erkannten Fehlerfall wird für die Bestimmung des Hubwinkels auf einen anderen, intakten Kanal logisch umgeschaltet (rekonfiguriert).

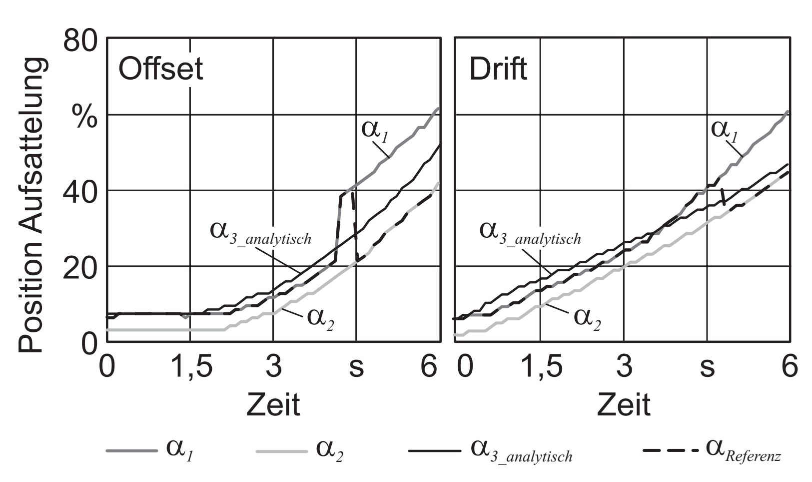


***Bild 7-4:** Fehlertolerante Positionserfassung der Drillenaufsattelung. Das fehlerhafte Signal wird durch Vergleich dreier Residuen ermittelt und der maßgebliche Referenzsensor rekonfiguriert. Dargestellt ist die Rekonfiguration vom α_1 auf α_2 wegen Offset- bzw. Driftfehler des defekten Sensors 1 beim Ausheben.*

Im dargestellten Versuch ist die Zeitspanne vom Auftreten des provozierten Fehlers bis zum Wirksamwerden der Sicherheitsfunktion 0,5 s. Diese Zeit muss im Ernstfall unterhalb der Fehlertoleranzzeit (Fehlerauftreten bis zum kritischen Zustand) der betreffenden Anwendung liegen. Die Fehlertoleranzzeit für einen Sensorfehler der Drillenaufsattelung liegt im Bereich von wenigen Sekunden, in denen ein Versagen des Aushubs u. U. zu

sicherheitskritischen Zuständen führen könnte, z. B. ausgelöst durch zu geringe Lenkkräfte an der Vorderachse.

Im Anwendungsbeispiel der automatisierten Traktor/Geräte-Kombination wurden unterschiedlichste Möglichkeiten angedacht, vorhandene Betriebs- und Schnittstellenzustände analytisch durch die erfassbaren Signale und Systemvariablen herzuleiten. Dazu findet man eine Übersicht im Anhang 9.2.

7.1.3 Konkurrierende Zugriffe auf Systemressourcen

Komplexe Arbeitsprozesse bei mobilen Arbeitsmaschinen erfordern paralleles Arbeiten unterschiedlicher Teilsysteme, die häufig auf gleichartige Leistungsressourcen der Hauptmaschine zurückgreifen müssen. Stoßen die verfügbaren Ressourcen an ihre Kapazitätsgrenze oder schließen sich die geforderten Sollwerte gegenseitig aus, müssen die konkurrierenden Zugriffe sicherheitsgerecht gelöst werden. Dieses kann sowohl bei abgeschlossenen mobilen Maschinensystemen mit hohem Automatisierungsgrad als auch bei automatisierten offenen Systemen mit anschließbaren Geräten notwendig sein. Hier behandelte Beispiele sind zum einen mehrere hydraulische Verbraucher, die mit einem begrenzt verfügbaren Gesamtvolumenstrom der hydraulischen Hauptpumpe auskommen müssen, zum anderen unterschiedliche Geschwindigkeitswünsche[1)] der landwirtschaftlichen Geräte des Versuchsträgers nach dem Prinzip „Gerät steuert Traktor“. Die Versuchsreihen zum Nachweis der Überwachung konkurrierender Zugriffe auf Systemressourcen beschränken sich auf diese zwei allgemein nutzbaren Ressourcen des Traktors und werden jeweils durch den Geltungsbereich des Überwachungsorgans (übergeordnet/untergeordnet) und die Verteilung der Prioritäten auf die Teilnehmer (gleichberechtigt/fest priorisiert/dynamisch priorisiert) unterschieden. Beispielsweise kann der **übergeordnete** Traktorrechner Ressourcen auf **untergeordnete** Geräte zuteilen und diese dann **gleichberechtigt** bedienen. Andererseits bestimmt ein Geräterechner **untergeordnet** die **feste Priorität** seiner eigenen hydraulischen Verbraucher.

7.1.3.1 Konflikte beim gemeinsamen Zugriff auf den hydraulischen Ölstrom

Wie im Kapitel 6.3.2 beschrieben, besteht bei hydraulischer Unterversorgung mehrerer Verbraucher die Gefahr der Verlangsamung der hydraulisch meist belasteten Verbraucher bis hin zum völligen Stillstand. **Bild 7-5** zeigt ein Beispiel für hydraulische Unterversorgung anhand der Aufsattelung der Drillmaschine mit herkömmlicher Differenzdruckregelung **ohne** „elektronisches LUDV“.

---

1) Auch der an den Traktorrechner gestellte spezifische Geschwindigkeitswunsch ist ein Zugriff auf die gemeinsam nutzbare Systemressource Fahrgeschwindigkeit.

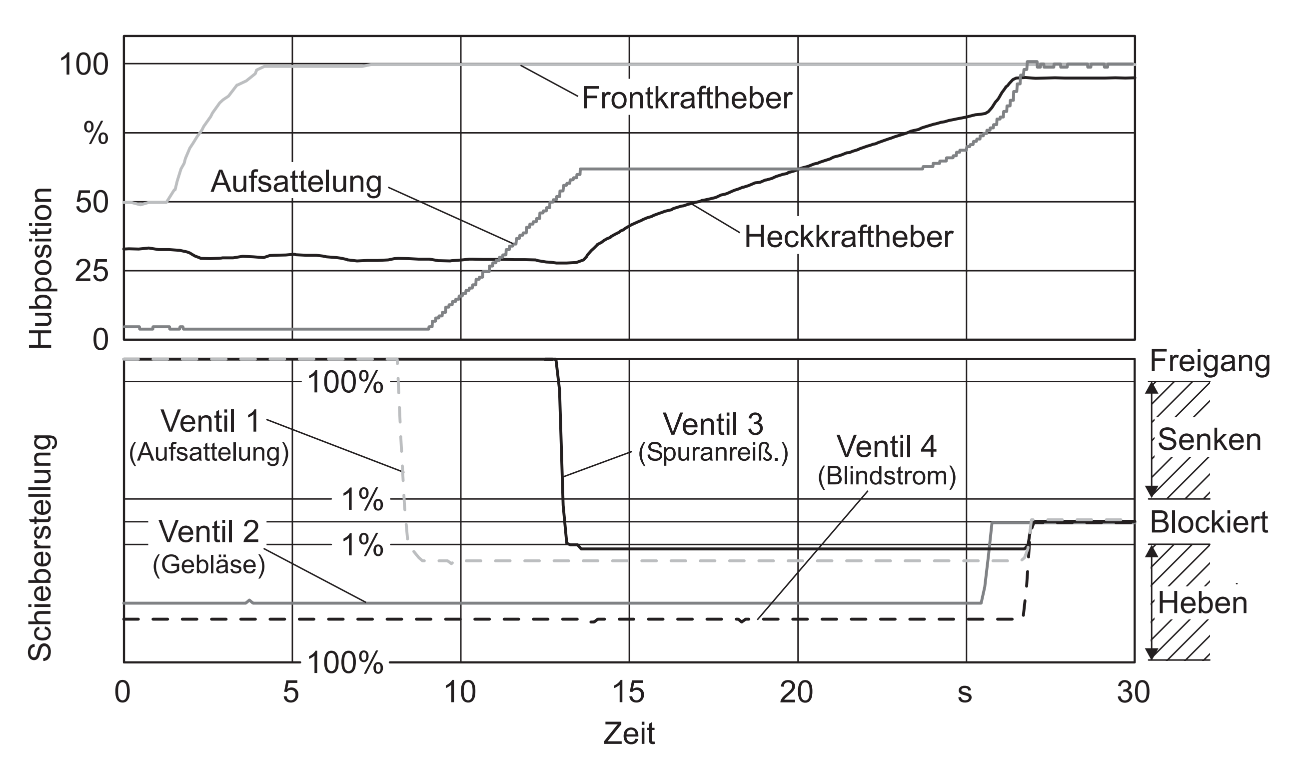


Bild 7-5: *Unterversorgung der Aufsattelung der Drillmaschine (Ventil 1) durch zeitgleiche Beschaltung der übrigen Ventile. Das Ausheben der Drillmaschine und des Heckkrafthebers wird deutlich verlangsamt (geforderte bzw. eingeprägte Volumenströme: Q_{V1} = 8 l/min, Q_{V2} = 30 l/min, Q_{V3} = 2 l/min, Q_{V4} = 40 l/min, Q_{FKH} = Q_{HKH} =77 l/min).*

Im dargestellten Versuch wurde, zusätzlich zum Antrieb des Gebläses der Drillmaschine über Ventil 2, ein weiterer dauerbestromter hydraulischer Verbraucher über eine am Ventil 4 angeschlossene Verstelldrossel simuliert, um die Kapazitätsgrenze der hydraulischen Pumpe leichter zu erreichen. Ausgelöst durch das Ausheben des Heckkrafthebers gerät das System zum Zeitpunkt 13 s bei einem geforderten Gesamtvolumenstrom[1)] von 157 l/min mit 47 l/min über dem verfügbaren Ölstrom in Unterversorgung. Die Aufsattelung kommt zum Stillstand und der Heckkraftheber verlangsamt gleichzeitig seine Bewegung, wodurch ein sicherheitskritischer Fehlerzustand auf Grund zu geringer Seitenführungskräfte an der Vorderachse verursacht wird. Das erneute Anfahren der Aufsattelung nach 23 s liegt an der Verringerung der Zylinderkraft durch Ausheben des Gesamtsystems über das Heckhubwerk (Verkürzung des Hebelarms). Erst mit standardmäßigem Abschalten des Gebläseantriebs (Ventil 2) entspannt sich endgültig die Situation.

In **Bild 7-6** ist nun das Verhalten des gleichen Systems mit elektronisch geregelter Durchflussverteilung gezeigt, wie es für das Versuchsgespann entwickelt und realisiert wurde, siehe auch Kapitel 6.3.2. Wieder wurde die an Ventil 4 angeschlossene Verstelldrossel mit 40 l/min versorgt und die übrigen Ventile durch geräteseitige Befehle wie im

1) Die eingeprägten Ölstromwerte der Hubwerke wurden mit 77 l/min empirisch aus Versuchen gewonnen und gelten für Motornenndrehzahl, welche durch die Automatik eingestellt wird.

vorigen Beispiel beaufschlagt. Im Falle der drohenden Unterversorgung der Ventile durch Überschreiten der maximal verfügbaren, von der Motordrehzahl abhängigen Ölvolumenstrom, werden die angeforderten Durchflüsse der Ventile zu verhältnismäßig gleichen Teilen vom Traktorrechner reduziert. Die Lösung des Konflikts läuft damit **übergeordnet gleichberechtigt** ab.

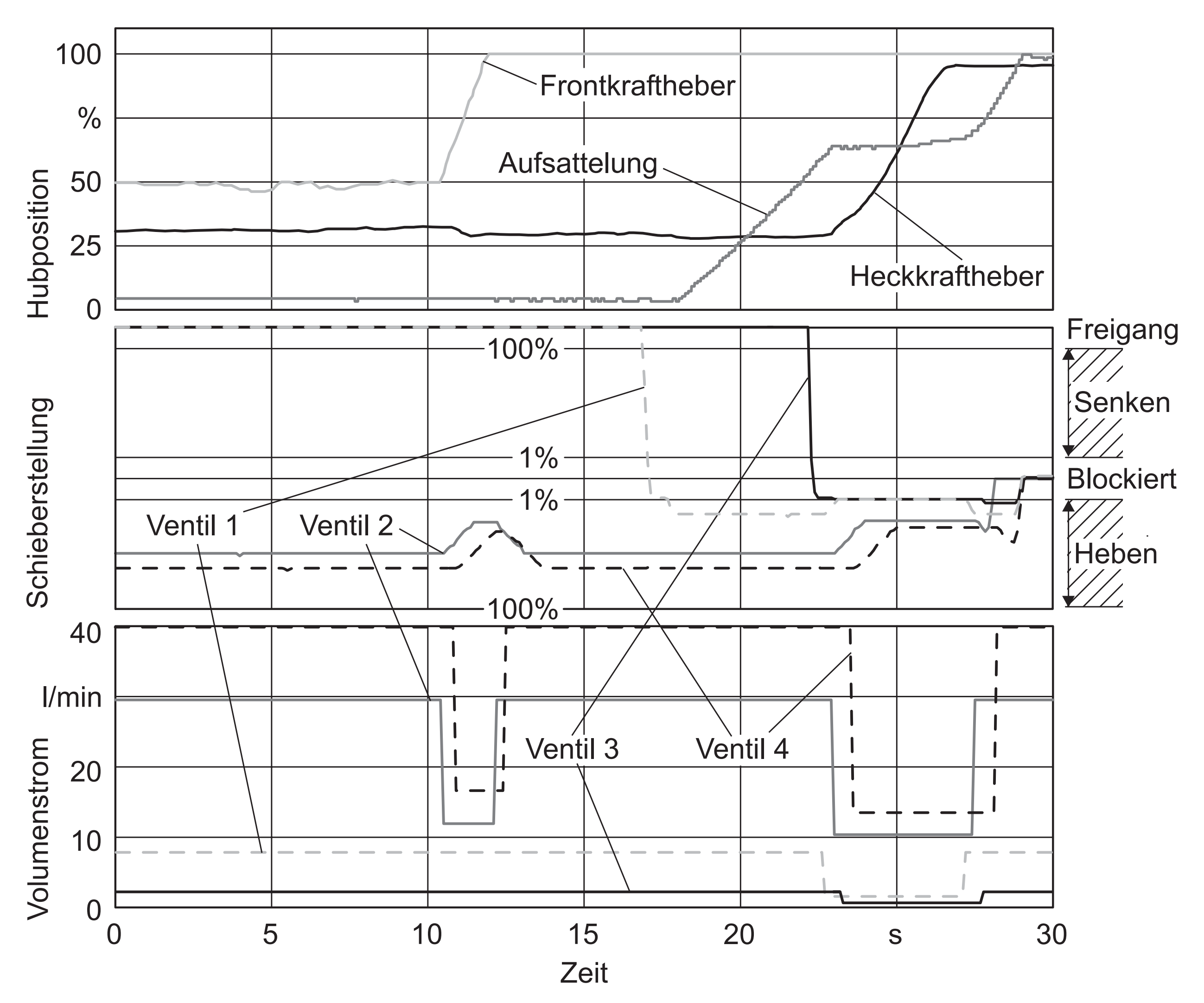


Bild 7-6: *Soziale Durchflussverteilung für die Zusatzventile bei Unterversorgung. Der Traktorrechner erkennt den Mangel an Volumenstrom und verteilt die Ressourcen gerecht auf die bestromten Ventile. Auch der höchstbelastete Verbraucher (Aufsattelung, Ventil 1) wird somit weiterhin versorgt und vor dem Stillstand bewahrt.*

Beim Zeitpunkt 10 s kommt zu den dauerbestromten Ventilen 2 und 4 die Betätigung des Frontkrafthebers (oberer Messschrieb) zum Ausheben des Ringpackers mit 77 l/min Ölstrom hinzu. Der bei entsprechender Drehzahl zur Verfügung stehende Volumenstrom von 110 l/min, wird dabei um 37 l/min überschritten. Für die Versorgung der Zusatzventile bleiben nur 33 l/min übrig. Um der Unterversorgung entgegen zu wirken, werden die Volumenströme der aktiven Ventile 2 und 4 jeweils automatisch um den Faktor $Q_{verfügbar}$/

$Q_{gefordert}$ (33/70) gemäß Formel (6-3) reduziert, unterer Messschrieb. Die Änderung des daraus resultierenden Schieberwegs der Ventile ist im mittleren Messschrieb gezeigt. Beim Ausheben des Heckkrafthebers zum Zeitpunkt 18 s werden die Auswirkungen gravierender: Jetzt ist zusätzlich das Ventil 1 zum Ausheben der Drillenaufsattelung mit 8 l/ min bestromt. Das Verhältnis $Q_{verfügbar}/Q_{gefordert}$ sinkt weiter und wieder müssen alle aktiven Ventile in ihrem Volumenstrom beschnitten werden. Als meist belasteter Verbraucher im hydraulischen System wird die sicherheitsrelevante Hubfunktion der Drillmaschine durch diese Maßnahme zwar verlangsamt, aber doch aufrechterhalten, siehe oberer Messschrieb. Wie beschrieben fallen die Hubwerke des Versuchsträgers aus systematischen Gründen nicht unter die automatische Volumenstromanpassung. Der Aufsattelvorgang verläuft deswegen im Vergleich zum Normalbetrieb, ohne zusätzlichen Verbraucher am Ventil 4, immer noch leicht verzögert ab (treppenförmiger Verlauf). In einer Serienlösung sollten jedoch sämtliche Verbraucher der Arbeitshydraulik berücksichtigt werden, wodurch die betrachteten Volumenstromeinbußen dann nicht so groß ausfallen würden.

Eine weitere Möglichkeit, den Zugriffskonflikt zu lösen, besteht in der **untergeordneten Priorisierung** sicherheitskritischer, hydraulischer Verbraucher intern durch den Geräterechner. Im Beispiel der automatisierten Gespannkombination wurde auch diese Alternative untersucht, **Bild 7-7**: Der elektronische Steuerrechner der Drillmaschine sensiert den drohenden Stillstand der Aufsattelkinematik bei einem Wert der Hubgeschwindigkeit kleiner als 1% pro Sekunde (siehe Zeitpunkt 27 s) und schaltet die sicherheitstechnisch unkritische, weniger wichtige Gebläsefunktion ab (Ventil 2 auf Blockiert).

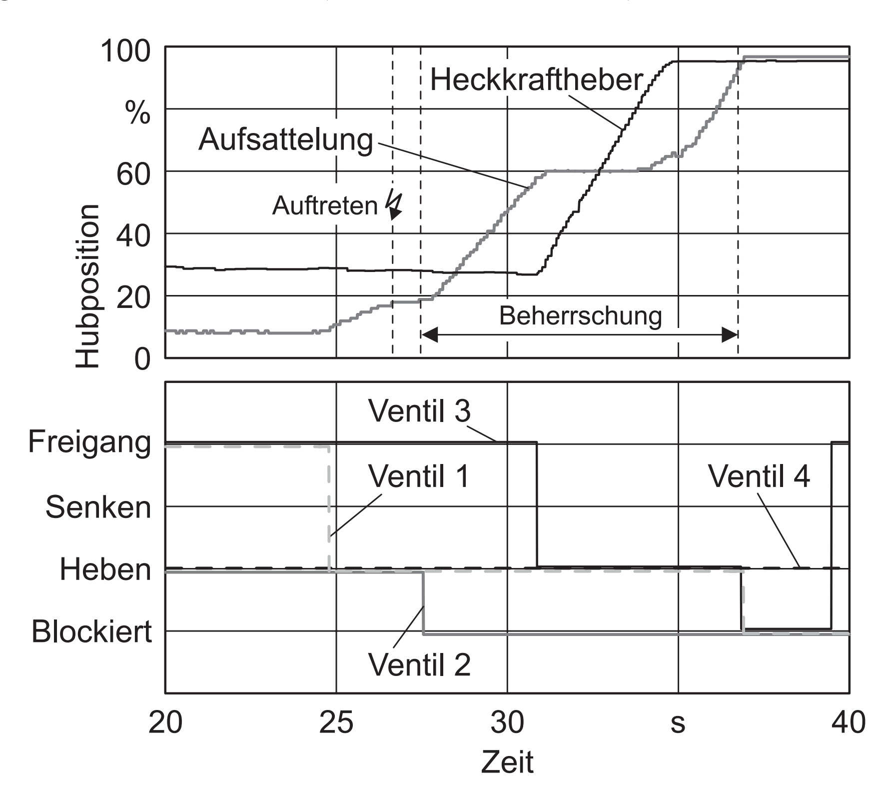


Bild 7-7: *Fail-Safe-Funktion durch Abschalten eines niederprioren Verbrauchers der Drillmaschinen durch ihren Steuerrechner. Das Ventil für das Gebläse (Ventil 2) wird auf Grund des detektierten Fehlers (Stillstand der Aufsattelung als priorisierte Sicherheitsfunktion) abgeschaltet. Die Aufsattelung wird damit sichergestellt.*

Die Priorisierung von Verbrauchern kann nur durch Instanzen erfolgen, welche die sicherheitstechnische Rangfolge der hydraulischen Funktionen objektiv beurteilen können. In diesem Beispiel regelt die Steuereinheit der Drillmaschine untergeordnet beide Funktionen für Aufsattelung und Gebläse und kann somit eindeutig entscheiden, welche Vorrang haben muss. Liegen die Funktionen nicht im Verantwortungsbereich **eines** Rechners ist die Priorisierung schwieriger. Auch der Traktorrechner als übergeordnetes Kontrollorgan kann alleine nicht entscheiden, welches der gleichberechtigten Geräte er bevorzugen soll. Eine weitere, nicht automatisch selbst konfigurierende Maßnahme wäre die Bildung einer fest zugewiesenen Rangliste durch den Fahrer. Bei dieser übergeordneten festen Priorisierung liegt es in der Verantwortung des Fahrers, die Wichtigkeit der Funktionen auch bei komplexen Zusammenhängen sicherheitstechnisch objektiv zu beurteilen.

Eine viel versprechende Möglichkeit für die sicherheitsgerechte Verteilung des hydraulischen Ölstroms ist die Mischform aus übergeordneter gleichberechtigter Volumenstromverteilung mit Priorisierung der wichtigsten sicherheitsrelevanten Verbraucher, denen ein Mindeststrom zugesichert wird.

7.1.3.2 Konflikte beim gemeinsamen Zugriff auf die Soll-Geschwindigkeit

Die Lösung konkurrierender Zugriffe auf die allgemeine Ressource Fahrgeschwindigkeit erfolgt **übergeordnet**, **dynamisch priorisiert** durch den Traktorrechner, **Bild 7-8**. Der Traktorrechner bestimmt die Rangordnung der Geschwindigkeitsanfragen je nach Arbeitszustand des anfragenden Gerätes und Ist-Zustand der Automatik. Anhand des obersten Messschriebs wird deutlich, in welchem Modus die Traktor/Geräte-Kombination arbeitet: Ist der Heckkraftheber und die Drillenaufsattelung ausgehoben (100 %), befindet man sich im Wendemodus, gleichbedeutend mit dem nach ISO 11783 definierten Zustand „Work“, bei abgesenkten Hubwerken im Automatikbetrieb der Reihenfahrt. Die Sollwertvorgaben der Geräte sind bei aktivem Automatikbetrieb gleichberechtigt. Außer der Kreiselegge haben die Geräte nach erfolgtem Einsetzen, d. h. bei normaler Reihenfahrt, keine Geschwindigkeitswünsche an den Traktor. Der jeweilige Sollwert wird in diesem Fall mit „don’t care“ belegt. Der Traktorrechner wählt aus den Soll-Geschwindigkeiten (unterer Messschrieb) die **niedrigste** gültige aus und regelt diese über die Übersetzungsverstellung am Traktor ein (mittlerer Messschrieb). Der Fahrer hat höchste Priorität und kann die Geschwindigkeitsregelung jederzeit übersteuern. Im Wendemodus wird die Geschwindigkeit alleine durch den Fahrer bestimmt – bei Wendeautomatik zusätzlich durch den Taskcontroller.

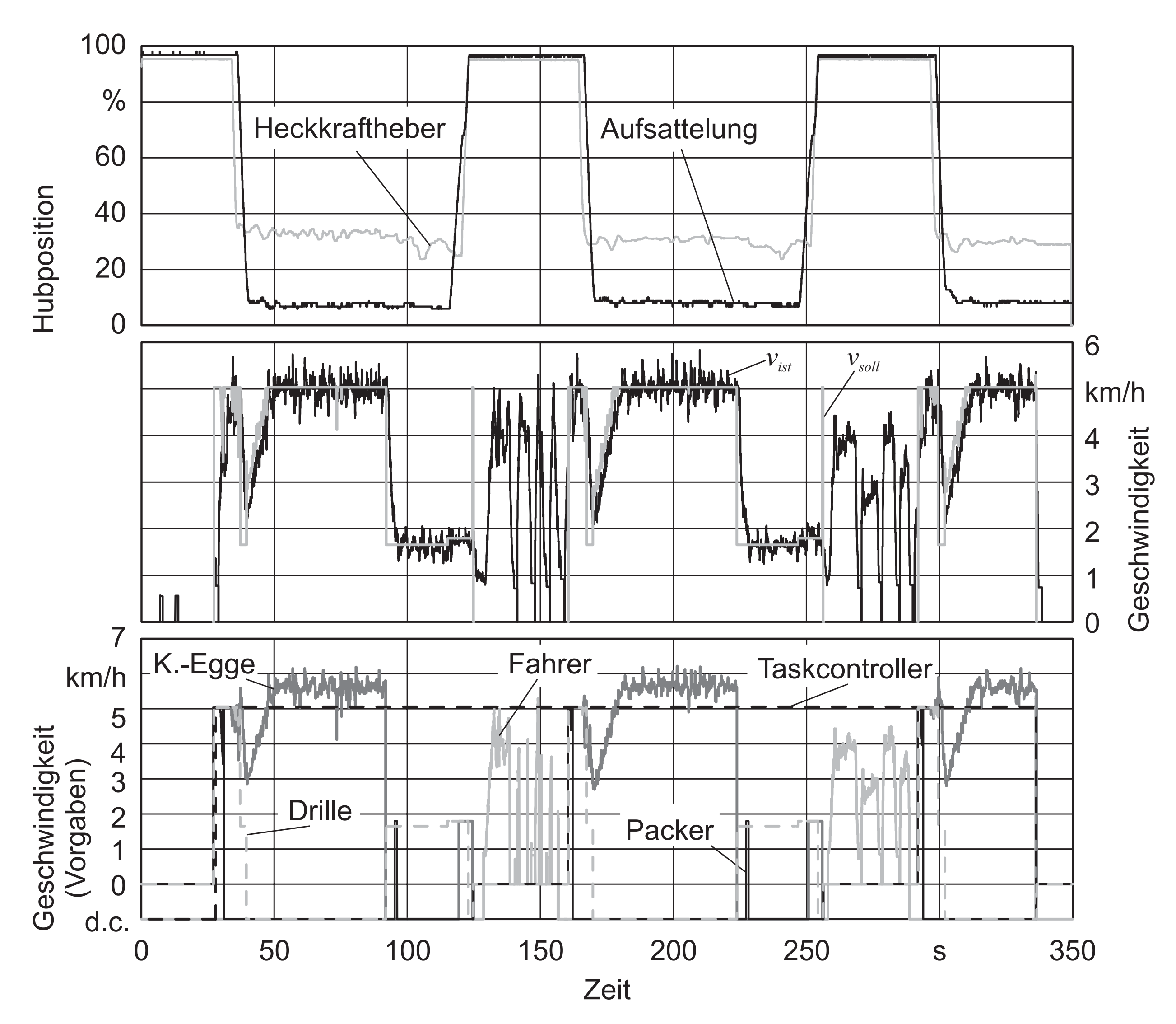


***Bild 7-8:** Priorisierung der niedrigsten gültigen Geschwindigkeit aus den Sollwertvorgaben der Geräte und des Taskcontrollers. Die priorisierte Geschwindigkeit v_{soll} wird vom Traktorrechner eingeregelt. Der Geschwindigkeitswunsch des Fahrers hat höchste Priorität. Dargestellt sind zwei Reihenfahrten mit Einsetzen und Ausheben am Vorgewende sowie die Wendevorgänge (ohne Wendeautomatik, Hubposition beim Wenden ca. 100%).*

7.1.3.3 Fazit

Zusammenfassend zeigt **Tabelle 7-1** allgemein gültige, unterschiedliche Strategien zur Lösung konkurrierender Zugriffe auf System-Ressourcen und nennt die wichtigsten Vor- und Nachteile der Ansätze. Die Art der Ressource, die hinsichtlich Zugriffs mehrerer Teilnehmer überwacht werden soll, hat großen Einfluss auf die gewählte Strategie, z. B. bietet sich für die Regelung von Geschwindigkeitsanfragen grundsätzlich eine dynamische Priorisierung abhängig vom Systemzustand der Automatiken an.

Tabelle 7-1: *Ansätze für die Konfliktlösung konkurrierender Zugriffe auf Systemressourcen. Unterschieden ist nach Geltungshorizont des Überwachungsorgans (übergeordnet bzw. untergeordnet) und Verteilung der Prioritäten auf die Teilnehmer (gleichberechtigt, fest priorisiert, dynamisch priorisiert).*

Lösung des Konflikts	Beispiel	Vorteile/Nachteile
übergeordnet gleichberechtigt	bei Unterversorgung gerechte Zurücknahme des Ölflusses durch den Traktorrechner, siehe auch Bild 7-6	+ alle Anfragen werden bedient + objektive Entscheidung – abhängig von Gesamtkapazität – Einschränkung aller Funktionen
übergeordnet mit fester Priorisierung	festgelegte Rangordnung hydraulischer Verbraucher durch den Fahrer	+ Sicherheitsfunktion verfügbar + objektive Entscheidung – Ausfall niederpriorer Funktionen – Priorisierung u. U. schwierig
übergeordnet mit dynamischer Priorisierung	zustandsabhängige Priorisierung der niedrigsten Soll-Geschwindigkeit der Geräterechner durch den Traktorrechner, siehe Bild 7-8	+ teilnehmerunabhängig + Eignung für allg. Ressourcen – alle abhängig vom Priorisierten – nur einfache Zusammenhänge
untergeordnet gleichberechtigt	bei Unterversorgung gerechte Zurücknahme des Ölflusses durch den Geräterechner (mehrere Verbraucher auf dem Gerät)	+ alle Anfragen werden bedient + kein Einfluss auf andere – subjektive Entscheidung – Effektivität in der Anwendung
untergeordnet mit fester Priorisierung	Abschalten niederpriorer Verbraucher durch das Gerät selbst (mehrere Verbraucher auf dem Gerät), siehe Bild 7-7	+ Sicherheitsfunktion verfügbar + kein Einfluss auf andere – Ausfall niederpriorer Funktionen – Effektivität in der Anwendung
untergeordnet mit dynamischer Priorisierung	konkurrierende Geschwindigkeitswünsche auf einem Gerät, nur ein Sollwert wird an den Traktorrechner gestellt	+ modulunabhängig + kein Einfluss auf andere – subjektive Entscheidung – Effektivität in der Anwendung

7.2 Koordination von Bewegungsabläufen

Bei vielen Arbeitsprozessen greifen komplexe Bewegungsvorgänge unterschiedlicher Geräte oder Werkzeuge zeitlich und räumlich ineinander. Andere Maschinen haben nur ein Werkzeug oder Gerät im Einsatz, der Arbeitsbereich und die kinematischen Bewegungsräume der Applikation teilen sich aber den Raum mit der Trägermaschine. Bei diesen Konstellationen ist die Gefahr groß, dass Teile des Maschinensystems miteinander oder mit Teilen ihrer Umgebung kollidieren. Die kritischen Zustände können dabei durch Fehler bei den automatisierten Bewegungsabläufen oder manuelle Betätigungsfehler hervorgerufen werden. Die MSR-Sicherheitsfunktionen haben in diesen Fällen die Aufgabe, manuell geschaltete und automatisierte Bewegungsabläufe zu überwachen und Kollisionen zu vermeiden. Beispiele sind elektronische Anschläge hydraulischer Bewegungsfunktionen von Baumaschinen, die die Bahnkurven der Werkzeuge überwachen, oder die im

Folgenden angesprochenen Sicherheitsabfragen, die beim verwendeten Versuchsträger realisiert wurden:

Koordination von **Heckkraftheber und Zapfwellenschaltung**: Eine einfache Möglichkeit, um eine zu große Kröpfung der Gelenkwelle zu vermeiden, ist in modernen Traktoren teilweise schon Standard. Dabei wird die Zapfwelle beim Senken des Heckkrafthebers erst ab einer vom Fahrer festgelegten Hubposition automatisch zugeschaltet. Im Anwendungsbeispiel „Gerät steuert Traktor" wurde die Überwachung erweitert: Beim Einsetzen übermittelt der Steuerrechner der Kreiselegge selbständig das Einschaltkommando der Zapfwelle an den Traktorrechner, abhängig von der Hubposition. Beim Ausheben wird zusätzlich die minimale Ausschalthöhe sichergestellt, die ein Stopfen wegen stillstehender Zinken im Boden verhindert.

Koordination von **Aufsattelung und Heckkraftheber**: Für den ordnungsgemäßen Aushub der Geräte am Feldende ist es nötig, das Ausheben des Heckkrafthebers erst dann zu beginnen, wenn die Aufsattelung der Drille eine gewisse Hubhöhe (60%) erreicht hat und der Hebelarm dadurch verkürzt wurde. Geschieht das nicht, sinkt die vordere Achslast und damit auch die aufbringbaren Seitenführungskräfte an der Vorderachse, trotz Ballast des Ringpackers, dramatisch. Der Rechner der Kreiselegge überwacht die Position der Aufsattelung und wartet die besagte Schwelle ab. Im Bild 7-8 ist die dem Start der Aufsattelung zugeordnete Hubhöhe des Heckkrafthebers von 60% erkennbar.

Koordination von **Frontkraftheber und Heckkraftheber**: Nach erfolgtem Einsetzen des Ringpackers durch den Frontkraftheber ergibt sich eine ähnliche Problematik wie beim Aspekt zuvor: Durch den schwimmend geführten Ringpacker fehlt bei ausgehobener Kreiselegge der Ballast an der Traktorfront, wodurch die Seitenführungskräfte an der Vorderachse sinken. Eine spezielle MSR-Sicherheitsfunktion des Packers wartet mit dem Einsetzen auf den Arbeitsbeginn der Kreiselegge. Erst dann sendet der Packer das Kommando bezüglich Absenkens des Frontkrafthebers an den Traktorrechner. Man verzichtet somit auf den punktgenauen Arbeitsbeginn des Packers, das heckseitige Hubmoment wird aber von Traktor und Ringpacker ausgeglichen. Denkbar wäre auch ein teilweises Absenken des Frontkrafthebers bis zu einem gewissen Tragdruck, um schon am Arbeitsbeginn eine oberflächliche Bearbeitung des Bodens bei verbleibender Ballastwirkung zu gewährleisten. Ist der Traktor dann heckseitig entlastet, kann der Ringpacker komplett abgesenkt werden und mit der Bearbeitung der tieferen Schichten beginnen.

Überwachung der **Stellung der Spuranreißer beim Wendevorgang**: Während der Reihenfahrt markiert der jeweils seitlich abgesenkte Spuranreißer eine parallel zur Fahrtrichtung verlaufende Linie im Ackerboden, die dem Fahrer eine Peilhilfe für die Rückfahrt bietet und ein genaueres Anschlussfahren ermöglicht. Nach dem Ausheben der Geräte beim Wendevorgang am Feldende ist es wichtig, den Spuranreißer in ausgehobene

Position zu bringen, um eine Kollision mit Hindernissen zu vermeiden. In der automatisierten Traktor/Geräte-Kombination überwacht deshalb die Kreiselegge den Zustand der Geräte und des Traktorrechners. Befindet sich die Kreiselegge im Zustand Wenden und sind die Meldungen der anderen Teilnehmer dazu plausibel, wird der Spuranreißer ausgehoben und durch Sperren eines Sitzventils vor unbeabsichtigtem Absenken gesichert. Die Spuranreißerfunktion wird allerdings wegen des aufkommenden GPS-gesteuerten Anschlussfahrens an Bedeutung verlieren.

7.3 Sicherheitsgerechtes Verhalten der Teilsysteme im Fehlerfall

Die notwendigen Aufgaben für die funktionale Absicherung des automatisierten Traktor/Geräte-Gespanns verteilen sich auf den Fahrer, die implementierten MSR-Sicherheitsfunktionen der Geräterechner und des Traktorrechners sowie die vorhandenen Vorkehrungen des serienmäßigen Fahrzeugrechners im Traktor. Im **Bild 7-9** ist die Aufgabenteilung zwischen Fahrer und elektronisch realisierten MSR-Sicherheitsfunktionen von der Systemüberwachung im Normalbetrieb bis zum Sicherheitseingriff im fehlerbeherrschenden Betrieb dargestellt.

Sicherheitskritische Zustände müssen durch den Fahrer oder die implementierten funktionalen Sicherheitssysteme erkannt werden. Danach liegt es in der Verantwortung des Fahrers und/oder der betreffenden MSR-Sicherheitsfunktionen, die notwendigen fehlerbeherrschenden Maßnahmen einzuleiten. Je nach Risikopotenzial reichen diese vom einfachen Eintrag des Fehlers in einen Fehlerspeicher für die spätere Auswertung in der Werkstatt bis zur fehlertoleranten Aufrechterhaltung der Funktion durch redundante Strukturen im Fail-Operational-System mit Warnmeldung an den Fahrer. Ziel aller Maßnahmen ist es, den sicheren Zustand des Systems nicht zu verlassen bzw. ihn noch vor Ablauf der Fehlertoleranzzeit einzuleiten. Der sichere Zustand der automatisierten Funktionen des Versuchsträgers kann stets durch Fail-Silent-Verhalten der Systeme sichergestellt werden, d. h. Abschalten der Regelung unter Warnmeldung und Übergabe der Kontrolle zurück an den Fahrer. Daraus resultieren die im Bild gezeigten Systemparameter für den sicheren Zustand. Herauszustellen ist hier die optionale Fail-Safe-Konfiguration für die Schaltung der hydraulischen Zusatzventile entweder auf Blockiert oder Freigang, konform zu ISO 11783 [117]. Je nach Anwendungsfall kann der sichere Betriebszustand eines hydraulischen Verbrauchers durch die Stellung Blockiert (z. B. Verhindern ungewollter Bewegungen eines Hubzylinders) oder auch Freigang (z. B. Vermeidung zu großer Massenkräfte beim abrupten Abschalten von rotierenden Systemen mit hoher Trägheit) definiert sein. Die Geräterechner übergeben den Fail-Safe-Schaltzustand ihrer zugeordneten Ventile als Konfigurationseinstellung an den Traktorrechner, wo sie zusammen mit den anderen Fail-

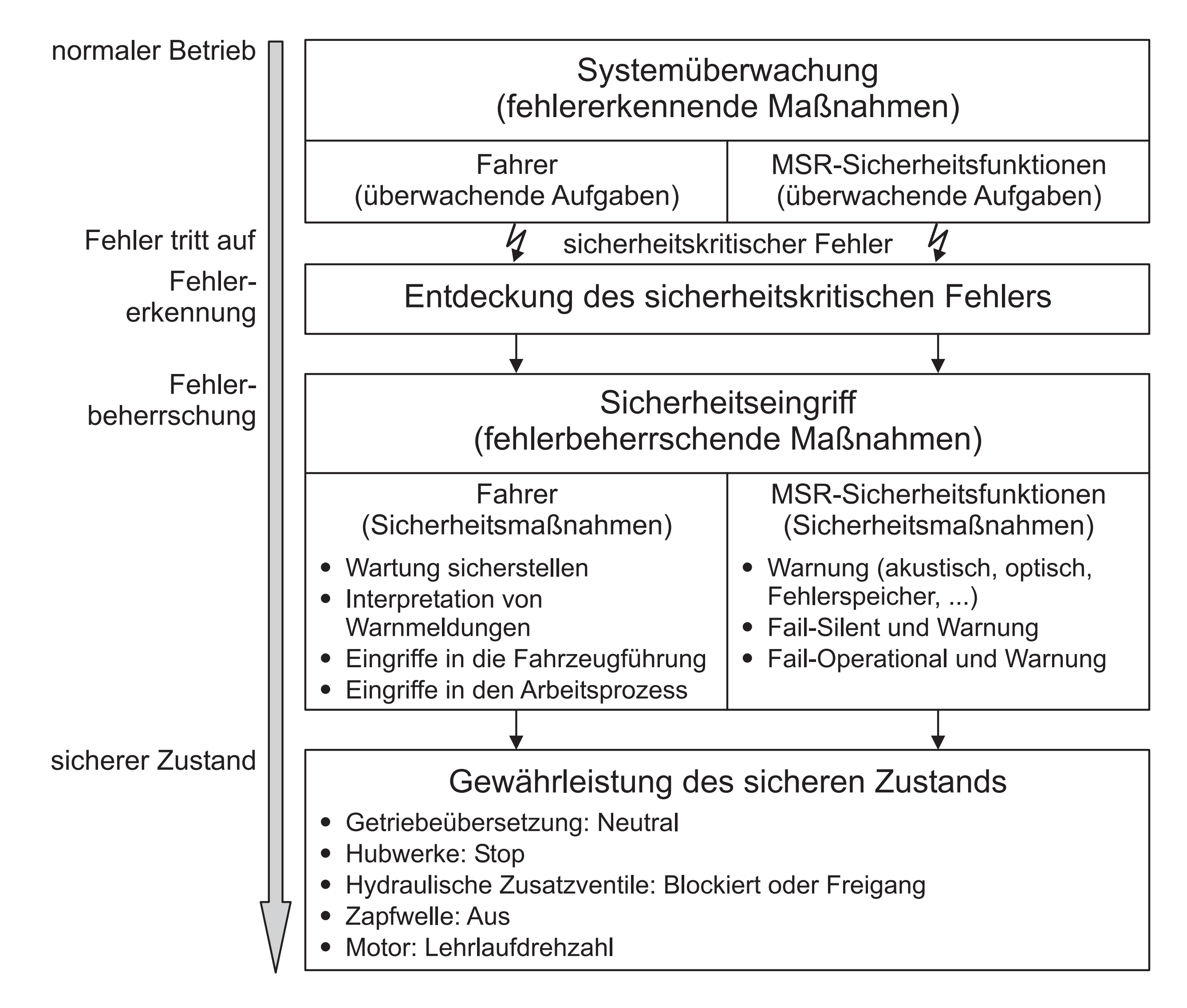
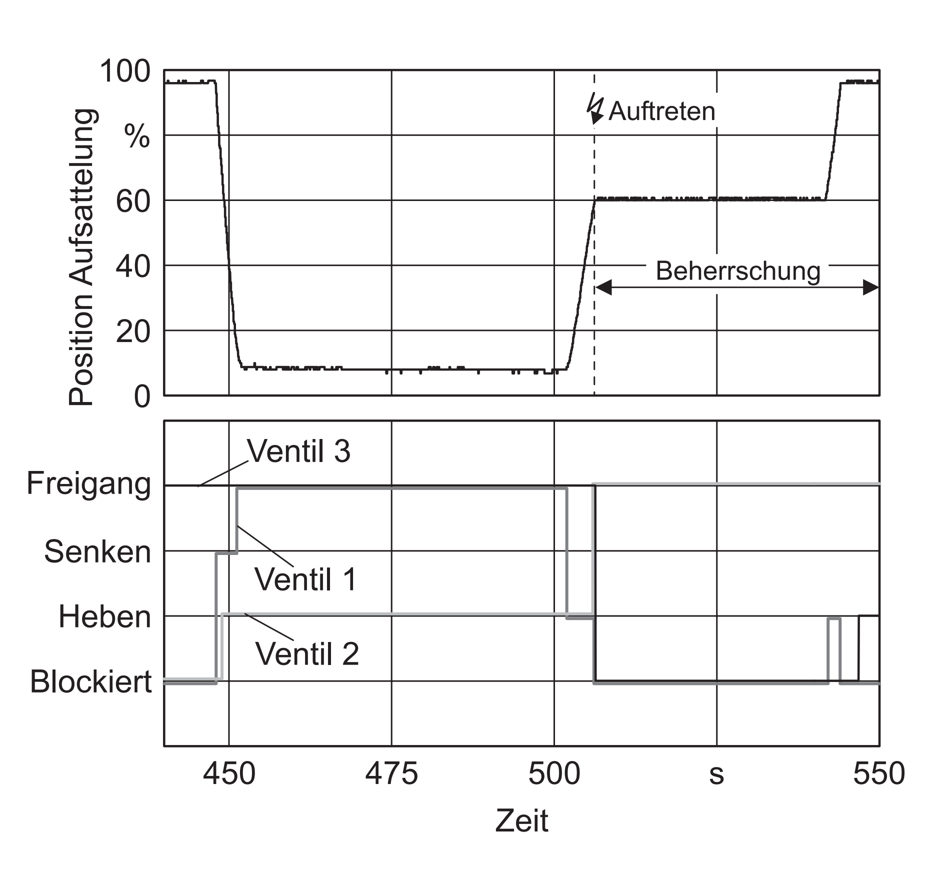


Bild 7-9: *Chronologischer Ablauf für fehlererkennende und -beherrschende Aufgaben des Fahrers und der MSR-Sicherheitsfunktionen im automatisierten Traktor/Geräte-Gespann.*

Safe-Einstellungen für Hubwerke, Antriebsstrang und Zapfwellen hinterlegt werden. Im Fehlerfall werden die Fail-Safe-Schaltvorgänge somit nicht durch Direktbefehle der Geräte, sondern aus Zeitgründen durch abgespeicherte Kommandos des Traktorrechners an den Traktor bewerkstelligt.

Bild 7-10 zeigt die Auslösung der Fail-Safe-Schaltung für die hydraulischen Zusatzventile nach Auftreten eines im Versuch provozierten, sicherheitskritischen Fehlers. Die Ventile der Hubvorrichtungen für die Aufsattelung der Drillmaschine (Ventil 1) und die Spuranreißer (Ventil 3) werden durch die Sicherheitsfunktion des Traktorrechners automatisch auf Blockiert geschaltet. Die Drehzahl des Gebläses der Drillmaschine soll im Fehlerfall jedoch kontrolliert herunterfahren. Die Fail-Safe-Stellung des Ventils 2 (Hydromotor des Gebläses) wurde deshalb vorher durch den Geräterechner der Drillmaschine auf Freigang konfiguriert und dementsprechend vom Traktorrechner eingestellt.

Bild 7-10: *Fail-Safe-Verhalten der hydraulischen Zusatzventile. Im Fehlerfall (bei 505 s) wird die Automatik abgeschaltet und die Ventile in den für sie vorher festgelegten sicheren Zustand gebracht. Auch nach dem Ausführen der Fail-Safe-Schaltung für die Ventile behält der Fahrer Handlungsgewalt (siehe manuelle Betätigung bei 540 s).*



7.4 Korrekte Interpretation und Verarbeitung des Fahrereingriffs

Der Fahrer der mobilen Arbeitsmaschine ist und bleibt vorerst noch wichtigstes Überwachungsorgan im Gesamtsystem. Auch wenn autonome, fahrerlose Konzepte, hauptsächlich aus dem Bereich der Landmaschinen (siehe Beispiel in [79]), die Machbarkeit von Vollautomatisierungen fahrerloser Fahrzeuge beweisen, ist der Aufwand einer kompletten Absicherung solcher Systeme enorm. Die überwachenden Tätigkeiten des Fahrers müssen durch genaue Erfassung interner und externer Fehlerzustände mittels aufwendiger Sensorik ersetzt werden. Speziell unvorhersehbare Ereignisse aus dem Maschinenumfeld sind schwer zu beherrschen. Da die Sicherheit, umgekehrt aber auch die Verfügbarkeit fahrerloser Systeme, meistens stark von der Anzahl der Sicherheitsabfragen abhängt, kann das Risikopotenzial bei angemessenem Aufwand und zufrieden stellender Zuverlässigkeit nur mit Verringerung des Schadenausmaß reduziert werden und nicht durch hochkomplexe und umfangreiche Sensorik. Will man fahrerlos autonome, mobile Arbeitsmaschinen realisieren, werden somit völlig neue Maschinenkonzepte angedacht werden müssen, z. B. kleine, langsame Einheiten mit dementsprechend wenig Gefährdungspotenzial.

Auch heutige Assistenzsysteme mobiler Arbeitsmaschinen arbeiten teilweise autonom bei Regelung des Arbeitsprozesses oder beim Eingriff in die Fahrzeugführung, binden aber den Fahrer in die Überwachung der Systeme mit ein. Beispiele sind an realen oder virtuellen Leitlinien geführte, automatische Lenksysteme. Der Fahrer wird mit diesen Sys-

temen entlastet, ist aber weiterhin als „Supervisor" erforderlich. Seine wichtigste Funktion ist es, vom System unerkannte Fehler oder kritische Zustände zu entdecken, bzw. auf Warnmeldungen des Systems zu reagieren. In [196] wird die Notwendigkeit aufgezeigt, die menschliche Zuverlässigkeit bei der Entwicklung von X-by-Wire-Systemen zu berücksichtigen, und eine Analysegrundlage für die Auslegung von komplexen Warnszenarios für den Fahrer gegeben. Wird der Fahrer darüber hinausgehend von automatisierten Eingriffen einer Sicherheitslogik bevormundet, z. B. durch autonome Eingriffe eines Kollisionsvermeidungssystems in Lenkung und Bremse, müssen diese Eingriffe wegen rechtlicher und produkthaftungstechnischer Gründe absolut ausfallsicher realisiert sein.

Im hier behandelten, automatisierten Versuchsgespann erfolgt die Regelung des Hauptarbeitsprozesses zwar autonom, der Fahrer muss aber jederzeit die vollständige Eingriffsmöglichkeit für Arbeitsprozess und Fahrzeugführung behalten. Um sicherheitskritische Zustände zu vermeiden, muss er innerhalb der Fehlertoleranzzeit auf einen Fehler aufmerksam gemacht werden, die Kontrolle über das System wieder übernehmen und den sicheren Zustand durch etwaige Maßnahmen gewährleisten können. Andererseits muss es dem Fahrer zugestanden sein, im eigenen Ermessen Systemparameter auch während des normalen Automatikbetriebs zu ändern. Sind die Eingriffe des Fahrers unkritisch für Sicherheit und Funktionalität der Automatik, wie z. B. die Verlangsamung der Fahrgeschwindigkeit, bleibt die Automatik vom Schreibrecht des Fahrers unberührt und arbeitet weiter. Im anderen Fall wird der Fahrer auf seinen funktions- oder sicherheitskritischen Eingriff durch Auslösen des Fail-Safe-Verhaltens aufmerksam gemacht, d. h. die Automatik stoppt, der Fahrer behält aber weiterhin die Kontrolle über das Gespann. Ein Beispiel hierfür zeigt Bild 7-10: Nach Auslösen des Fail-Safe-Verhaltens ist der Fahrer in der Lage, durch manuelles Schalten des Ventils 1 zum Zeitpunkt 540 s die Aufsattelung der Drillmaschine zu betätigen und somit auf die Situation zu reagieren. Ein weiteres Beispiel ist der Eingriff des Fahrers auf die Geschwindigkeit während des Automatikbetriebs: Solange keine Limits oder aktuellen Sollwerte der Geräte oder des Taskcontrollers überschritten werden, kann der Fahrer die Geschwindigkeit bedarfsweise erhöhen. Bei Überschreiten der Grenzwerte wird aber wegen drohender Beschädigung der Geräte oder Nichterreichen der funktionellen Vorgaben der Fail-Safe ausgelöst.

8 Zusammenfassung

Der Anteil elektronisch geregelter Systeme bei mobilen Arbeitsmaschinen nimmt wie in anderen Bereichen der Fahrzeugtechnik stetig zu. Zusätzlich zum Eingriff in den Antriebsstrang werden auch die Arbeitsprozesse von einem immer höheren Automatisierungsgrad geprägt. Die verwendeten Technologien der Systeme und das Fehlen konventioneller Rückfallebenen stellen neue Anforderungen an ihre Betriebssicherheit. Die Ausfallsicherheit wird oftmals nicht mehr durch einzelne Bauteilzuverlässigkeiten festgelegt, sondern von den Zuverlässigkeiten der elektronifizierten Elemente, bestimmt durch Hardware und Software. Gerade bei programmierbaren, mechatronischen Systemen liegt die Schwierigkeit in der Quantifizierung der Zuverlässigkeiten von Software oder komplexen elektronischen Systemen, insbesondere elektronischen Steuergeräten. Zentrale Intention der vorliegenden Arbeit ist die Bereitstellung eines sicherheitsgerechten Entwicklungskonzepts für mechatronische Systeme bei mobilen Arbeitsmaschinen, das den Nachweis der geforderten Systemzuverlässigkeit über ein dem Risikopotenzial angemessenes methodisches Vorgehen führt.

Der theoretische Hauptteil der Arbeit behandelt die Vorgehensweise und Methodenzuordnung des Entwicklungskonzepts in Abhängigkeit zur geforderten Systemintegrität. Das ausgearbeitete Konzept beginnt bei der sicherheitstechnischen Untersuchung des Gesamtsystems, wobei das Gefährdungspotenzial und damit der erforderliche Safety-Integrity-Level (SIL) ermittelt werden. Theoretische Untersuchungsmethoden wie Risikoanalyse und System-FMEA stehen dabei im Vordergrund und wurden an den Anwendungsfall „mobile Arbeitsmaschine im Arbeitseinsatz“ angepasst. Abhängig vom resultierenden SIL wird die passende Systemarchitektur ausgewählt und es werden die geeigneten Entwicklungsmaßnahmen und -methoden den einzelnen Entwicklungsschritten des erarbeiteten V-Modells zugeordnet. Als Alternative zur konventionellen Methodik werden die Vorteile einer durchgängig modellbasierten Entwicklung elektronischer Steuergeräte herausgearbeitet. Die Werkzeugkette Matlab/Simulink/Stateflow wurde dafür, von der Spezifikation einzelner Funktionen bis zur Generierung des fertigen Serien-Codes für das Steuergerät,

anhand einer durchgängig modellbasierten Vorgehensweise eingesetzt und mit konventionellen Methoden verglichen.

Der praktische Teil der Arbeit beschreibt den Versuchträger und die realisierten Automatiken, behandelt die Validierung der wichtigsten MSR-Sicherheitsfunktionen (Messen, Steuern, Regeln) und verallgemeinert die Ergebnisse auf das gesamte Segment der mobilen Arbeitsmaschinen. Für die Weiterentwicklung und Verifikation des Konzepts wurde eine geeignete Traktor/Geräte-Kombination als Versuchsträger ausgewählt. Der Traktor verfügt über elektronische Schnittstellen für Motor und stufenloses Getriebe und wurde wie die landwirtschaftlichen Geräte (Ringpacker, Kreiselegge und aufsattelbare Drillmaschine) mit zusätzlicher Sensorik und Elektronik ausgerüstet.

Die Entwicklung der Automatiken orientierte sich am erarbeiteten Konzept. Bei der autonomen Prozessführung nach dem Prinzip „Gerät steuert Traktor“ regeln die landwirtschaftlichen Geräte den Traktor in seiner Fahrgeschwindigkeit und Betätigung der hydraulischen bzw. mechanischen Schnittstellen (Zapfwelle, Hubwerke und Zusatzhydraulik) sowohl während der eigentlichen Arbeit als auch am Vorgewende. Als zweites Anwendungsbeispiel dient eine neu realisierte Wendeautomatik. Hierfür wird die Position relativ zum Wendebereich am Feldende aus Lenkwinkel und Geschwindigkeit ermittelt. Der übergeordnete Traktorrechner (Brückenrechner zwischen Traktor und Geräten) regelt den Wendevorgang des Gespanns hinsichtlich Motordrehzahl, Wendeschaltung und Geschwindigkeit – der Fahrer muss nur noch lenken.

Die entwickelten MSR-Sicherheitsfunktionen bezogen sich auf die Überwachung und Plausibilisierung sicherheitsrelevanter Prozessgrößen, die Regelung konkurrierender Zugriffe auf Systemressourcen und die Koordination von Bewegungsabläufen kinematischer Vorgänge. Signifikante Fallbeispiele sind eine elektronisch realisierte Durchflussverteilung bei drohender Unterversorgung der Arbeitshydraulik und eine fehlertolerante Sensorerfassung für die Aufsattelposition der Drillmaschine, die mit Hilfe analytischer Redundanz ein 3-kanaliges und damit ausfallsicheres System umsetzt.

Die Versuchsergebnisse und Erfahrungen ließen sich auf den gesamten Bereich der mobilen Arbeitsmaschinen verallgemeinern, wobei als Teilaspekte insbesondere das sicherheitsgerechte Verhalten der Teilsysteme im Fehlerfall und die korrekte Interpretation und Verarbeitung des Fahrereingriffs herausgearbeitet wurden.

9 Anhang

9.1 Bewertungskatalog System-FMEA (angepasst an mobile Arbeitsmaschinen)

Der entwickelte Bewertungskatalog dient als Vorlage, die vor Durchführung der FMEA im Team diskutiert und abgestimmt werden muss. Während der Bewertung ist es sinnvoll, den Katalog dynamisch mit Beispielen und Anmerkungen zu erweitern.

Tabelle 9-1: Bedeutung B *(Auswirkung): Trennung nach sicherheitsgerichteten (grau hinterlegte Felder) und qualitativen Kriterien (Funktionalität, Komfort)*

Wert	Beschreibung
1	**Kaum wahrnehmbar** *Sicherheit:* Keine Beeinträchtigung der Sicherheit *Einhaltung gesetzlicher Vorschriften:* Kein wahrnehmbarer Fehler *Kosten:* Keine Kosten
	Kaum wahrnehmbar *Funktionalität:* Keine funktionale Einschränkung des Systems *Komfort:* Keine Komforteinschränkung wahrnehmbar
2	**Gering** *Sicherheit:* Keine Beeinträchtigung der Sicherheit *Einhaltung gesetzlicher Vorschriften:* Fehler hat geringe Auswirkung auf gesetzliche Vorschriften, kann vom Fahrer behoben werden (z. B. Kennzeichen verschmutzt, Reinigung notwendig). *Kosten:* Der Fehler verursacht geringe Kosten (z. B. Austausch von Kleinteilen).
	Gering *Funktionalität:* Geringfügiger Fehler im System, der nicht sofort in der Werkstatt behoben werden muss. Fehlerbehebung im Regelservice möglich (z. B. Einstiegsleuchte defekt). *Komfort:* Fehler, durch den sich der Fahrer nur geringfügig belästigt fühlt (z. B. Innenbeleuchtung defekt, Zigarrenzünder defekt).

3	**Gering** *Sicherheit:* Keine Beeinträchtigung der Sicherheit. *Einhaltung gesetzlicher Vorschriften:* Fehler hat geringe Auswirkung auf gesetzliche Vorschriften und kann von technisch versiertem Fahrer behoben werden (z. B. Kennzeichenbeleuchtung nicht i. O., bedingt Lampenwechsel). *Kosten:* Der Fehler verursacht geringe Kosten (z. B. Austausch von Verschleißteilen).
	Gering *Funktionalität:* Geringe Funktionseinschränkung von Bedien- und Komfortsystemen; geringfügiger Fehler am Fahrzeug, der nicht sofort in der Werkstatt behoben werden muss. Fehlerbehebung im Regelservice möglich (z. B. Ausfall Außentemperaturanzeige) *Komfort:* Fehler, durch den sich der Fahrer geringfügig belästigt fühlt (z. B. Ausfall Sitzheizung, Ausfall des Staubfilters).
4	**Gering** *Sicherheit:* Geringe Beeinträchtigung der Systemsicherheit. Verletzung von Personen oder Schäden am System sind unter normalen Bedingungen auszuschließen (z. B. Ablenkung des Fahrers, erhöhte Betätigungskräfte, Außenspiegel wackelt). *Einhaltung gesetzlicher Vorschriften:* Fehler bedingt eine Nachbesserung in der Fachwerkstatt. *Kosten:* Der Fehler verursacht mittlere Kosten (z. B. Kraftstoffverbrauch zu hoch).
	Gering *Funktionalität:* Geringfügiger Systemfehler, der einen Werkstattaufenthalt bedingt (z. B. Tür schwergängig). *Komfort:* Fehler, durch den sich der Fahrer belästigt fühlt (z. B. Ausfall Klimaanlage).
5	**Mittelschwer** *Sicherheit:* Mittelschwere Beeinträchtigung der Systemsicherheit (u. a. bemerkter Ausfall einer Schutzfunktion). Geringes Risiko für Verletzungen von Personen bzw. Schäden am System (z. B. Motorbremsleistung nicht i. O.). *Einhaltung gesetzlicher Vorschriften:* Fehler bedingt Nachbesserung in der Fachwerkstatt (z. B. Schadstoffemission). *Kosten:* Der Fehler verursacht mittlere Kosten (z. B. aufwendige Diagnose).
	Mittelschwer *Funktionalität:* Funktionsfähigkeit des Fahrzeugs ist eingeschränkt. Mittelschwerer Fehler am Fahrzeug, der einen Werkstattaufenthalt bedingt (z. B. Drehmoment zu niedrig/hoch, zuwenig/zuviel Kraftstoff wird eingespritzt, Lack blättert ab). *Komfort:* Fehler, durch den sich der Fahrer belästigt fühlt; Funktionseinschränkung wichtiger Komfortsysteme (z. B. Ausfall der Heizung)

6	**Mittelschwer** *Sicherheit:* Mittelschwere Beeinträchtigung der Systemsicherheit (u. a. bemerkter Ausfall einer Schutzfunktion). Geringes Risiko für Verletzungen von Personen bzw. Schäden (z. B. Allrad, Differentialsperre nicht verfügbar obwohl angezeigt, Motor geht aus, Fahrzeug bleibt stehen). *Einhaltung gesetzlicher Vorschriften:* Fehler bedingt Ausbesserung in Fachwerkstatt (z. B. Abgaswerte nicht erfüllt, leichte Rußbildung, Lärmbelastung für die Umwelt). *Kosten:* Der Fehler verursacht mittlere Kosten
	Mittelschwer *Funktionalität:* Funktionsfähigkeit des Fahrzeugs eingeschränkt; mittelschwerer Fehler am System, der einen Werkstattaufenthalt bedingt (z. B. Fahrzeug zieht stark auf eine Seite, Ausfall von Teilsystemen wie die Tankanzeige). *Komfort:* Fehler, durch den sich der Fahrer belästigt fühlt; Funktionseinschränkung wichtiger Komfortsysteme (z. B. Fahrzeug lässt sich nicht abschließen, schlechte Arbeitsqualität).
7	**Schwer** *Sicherheit:* Grobe Beeinträchtigung, die eine Reduzierung der Systemsicherheit zur Folge hat. Fehler kann zur Verletzung von Personen oder erheblichen Beschädigungen des Systems führen (z. B. Teilausfall der Fahrbeleuchtung). *Einhaltung gesetzlicher Vorschriften:* Fehler führt zu Belastung der Umwelt und macht dringenden Werkstattaufenthalt erforderlich (z. B. starke Lärmbelastung für Fahrer, zu starke Rußbildung). *Kosten:* Fehler verursacht hohe Kosten (z. B. Tausch der Lichtmaschine).
	Schwer *Funktionalität:* Funktionsfähigkeit des Fahrzeugs stark eingeschränkt. Schwerwiegender Fehler, der ein Weiterarbeiten mit stark reduzierter Leistung oder anderen Einschränkungen verursacht. Eine Reparatur ist in jedem Falle erforderlich (z. B. Dreschen mit niedriger Geschwindigkeit). *Komfort:* Gewohnte Komfortleistungen sind ausgefallen bzw. stark eingeschränkt (z. B. Kabinenfederung/Sitzfederung defekt, starke Klappergeräusche).
8	**Schwer** *Sicherheit:* Grobe Beeinträchtigung, die eine Reduzierung der Systemsicherheit zur Folge hat. Fehler kann zur Verletzung von Personen oder erheblichen Beschädigungen des Systems führen (z. B. Bremskraftverstärker defekt, Fahrzeug beschleunigt ungewollt). *Einhaltung gesetzlicher Vorschriften:* Fehler führt zu Umweltverschmutzung und macht dringenden Werkstattaufenthalt erforderlich (z. B. starke Lärmbelastung für Fahrer, Luftverschmutzung, starke Rußbildung). *Kosten:* Fehler verursacht sehr hohe Kosten (z. B. Austausch von Teilsystemen).
	Schwer *Funktionalität:* Funktionsfähigkeit des Fahrzeugs stark eingeschränkt; schwerwiegender Fehler, der ein Weiterarbeiten mit stark reduzierter Leistung oder anderen Einschränkungen verursacht. Eine Reparatur ist in jedem Falle erforderlich (z. B. Fahrzeug im Notlauf mit stark verminderter Leistung, Getriebe nur im niederen Gang, Arbeitsstillstand). *Komfort:* Fehler, der eine Verärgerung des Fahrers auslöst. Komfortbereich wird verlassen. Erreichen der Schmerzgrenze (z. B. Heizung nicht abschaltbar, Fahrzeug bleibt stehen).

9	**Äußerst schwerwiegend** *Sicherheit:* Schwere Beeinträchtigung, die zu schweren Verletzungen von Personen od. zum Totalverlust des Systems führt (z. B. Bremsfunktion stark beeinträchtigt, Antriebswelle bricht, Ausfall der Servounterstützung). *Einhaltung gesetzlicher Vorschriften:* Grober Verstoß gegen die gesetzlichen Vorschriften (z. B. leichte Grundwasserverschmutzung, Umweltschaden). *Kosten:* Fehler verursacht erhebliche Kosten (z. B. Austausch Motor, Totalschaden).
	Äußerst schwerwiegend *Funktionalität:* Fehler, der zu einem Systemausfall bzw. Totalschaden führt (z. B. Totalschaden, Ausfall Kühlsystem, Motorschaden, Getriebeschaden).
10	**Äußerst schwerwiegend** *Sicherheit:* Schwere Beeinträchtigung, die zu schweren Verletzungen bzw. zum Tod von Personen führt od. zum Totalverlust das Systems (z. B. Ausfall der Bremse od. Lenkung, Motor beschleunigt ungewollt, Personenschaden). *Einhaltung gesetzlicher Vorschriften:* Grober Verstoß gegen die gesetzlichen Vorschriften (z. B. schwere Grundwasserverschmutzung, schwerer Umweltschaden). *Kosten:* Fehler verursacht erheblich Kosten (z. B. Umweltschäden, Regressforderungen).

Tabelle 9-2: *Die **Auftretenswahrscheinlichkeit A** bewertet die Wahrscheinlichkeit des Auftretens der Ursache unter Berücksichtigung aller wirksamen Vermeidungsmaßnahmen.*

Wert	Beschreibung
1	**Unwahrscheinlich** System mit langjähriger, schadensfreier Erfahrung. Vorab 100 %ige Prüfung.
2	**Sehr selten, einmal im Leben** Bewährtes System mit langjähriger Serienerfahrung ohne bekannte Fehlermeldungen.
3	**Selten** Bewährtes System, bewährte Auslegung mit Detailänderungen an bewährten Teilsystemen.
4	**Gering, einmal im Jahr** Bewährtes System mit Einsatz von Teilsystemen unter geänderten Bedingungen.
5	**Hin und wieder** System basiert auf früheren Entwicklungen und Variationen davon. (Bewährtes System mit neuen Teilsystemen)
6	**Gelegentlich, mehrmals im Jahr** Neues System beinhaltet Neuentwicklung mit Erfahrung bei vergleichbaren Anwendungen.
7	**Mäßig** Neues System unter Einsatz bisher teilweise problematischer Technologien. (Unausgereiftes Konzept)
8	**Erhöht, immer wiederkehrend** Neues System unter Einsatz neuer unerprobter Technologien. (Unausgereiftes Konzept, erschwerte Einsatzbedingungen)
9	**Hoch** Neuentwicklung ohne jegliche Erfahrung.
10	**Sehr hoch, praktisch bei jedem Einsatz** Innovative Systemauslegung mit nicht einschätzbaren Einsatzbedingungen.

Tabelle 9-3: *Die **Entdeckenswahrscheinlichkeit E** bewertet die Wahrscheinlichkeit für eine Entdeckung der Fehlerursachen vor Eintreten der Fehlerfolgen.*

Wert	Beschreibung
1	**Sehr hoch** Der Fehler wird sicher entdeckt. Fahrer entdeckt den Fehler und zusätzlich entdeckt das System einen Fehlerzustand und reagiert mit Gegenstrategie oder Anzeige für den Fahrer. Folgen können sicher vermieden werden (z. B. augenscheinlicher Fehler und automatische Prüfung mit Warnmeldung).
2	**Hoch** Der Fehler wird durch das System erkannt und es reagiert mit Gegenstrategie oder Anzeige/ Warnhinweis für den Fahrer. Fail-Operational-Verhalten (z. B. fehlertolerantes, redundantes System mit Warnmeldung)
3	**Gut** Augenscheinlicher Fehler – der Fehler wird durch den normal aufmerksamen Fahrer bemerkt. Fail-Silent-Verhalten (z. B. starke Geräusche, Ölflecken, mechanische Rückfallebene und Warnmeldung)
4	**Befriedigend** Der Fehler wird durch spezielle Fahrerprüfungen entdeckt (z. B. Kontrolle der Anzeigelampen, starke bis mittlere Niveauabweichung, verändertes Fahrverhalten,...).
5	**Mangelhaft** Der Fehler kann nur vom technisch versierten Fahrer entdeckt werden. Prüfung notwendig (z. B. geringe Niveauabweichung, geringer Leistungsverlust, leichte Geräuschentwicklung,...)
6	**Schlecht** Fehler wird routinemäßig im Wartungsdienst bemerkt, bzw. den Fahrer unterstützende Sensorik wäre notwendig. Fail-Silent-Verhalten ohne Warnmeldung (z. B. fehlerhafte Steckverbindung,...)
7	**Sehr schlecht** Der Fehler wird in der normalen Inspektion aufgrund der vorgeschriebenen Prüf- und Durchsichtsmaßnahmen erkannt (z. B. Undichtheiten).
8	**Gering** Der Fehler ist nur in der Werkstatt durch eine Prüfung zu entdecken (z. B. Kabelverbindung nur teilweise gesteckt).
9	**Sehr gering** Fehler ist nur durch spezielle Prüfungen oder Testabläufe zu entdecken (z. B. Stoßdämpfertest, Motortest).
10	**Unwahrscheinlich** Der Fehler wird nicht entdeckt. Der Fehler wird nur durch das Eintreten der Top-Fehlerfolge entdeckt.

9.2 Matrix analytisch herleitbarer Betriebs- und Schnittstellenzustände

Wichtige MSR-Sicherheitsfunktionen basieren auf Plausibilisierungen sicherheitsrelevanter Parameter oder der Herleitung von Signalen für analytische Redundanz. **Tabelle 9-4** zeigt eine Übersicht für analytisch herleitbare Betriebs- und Schnittstellenzustände, die aus zentral verfügbaren sensorisch erfassten oder rechnerisch bestimmten Größen gewonnen werden können. Die Übersicht wurde für den verwendeten Versuchsträger erarbeitet, hat aber Grundlagencharakter auch für andere Maschinensysteme.

***Tabelle 9-4:** Zusammenstellung von zentral erfassbaren Signalen zur analytischen Herleitung wichtiger Systemzustände. (h: hinreichende Bedingung, n: notwendige Bedingung, b: unter bestimmten Bedingungen, Indizes markieren abhängige Signalkombinationen)*

Arbeitshydr.				Zapfwelle			Betriebszust.				Fahrgeschwindigkeit						**Analytisch herleitbar** / Erfassbare Signale	
Hydromotor Drehzahl	Status Freigang	Zylinder Position	Kraftheber Position	Zapfwelle gekoppelt	Zapfwelle Moment	Zapfwelle Drehzahl	Ruhe-/Parkstellung	Arbeitszustand (Engage)	Arbeitszustand (Work)	Transportzustand	ab 13 km/h (Transport)	bis 13 km/h (Rangieren)	bis 13 km/h (Bestellung)	um 8 km/h (Grubber)	um 6 km/h (Fräse/Pflug)	Stand (Güllepumpe)		
n	n				b	h_1		n	n		h	h	h	h	h_1		Motordrehzahl	Antriebsstrang
											h_1	h_1	h_1	h_1	h_1	h_1	Getriebeübersetzung	
							h	n	n		n	n	n	n	n	h	Parksperre	
											n	n	n	n	n	h_1	aktiver Stillstand	
											h_1	h_1	h_1	h_1	h_1	h_1	Hauptfahrkupplung geschlossen	
							n/h				n/h	n/h	n/h	n/h	n/h	n/h	theoretische Fahrgeschwindigkeit	
							n/h				n/h	n/h	n/h	n/h	n/h	n/h	wahre Geschwindigkeit (Radar)	
			n				n/h	h	b				h	h	h	h	wahre Geschwindigkeit (Peiseler Rad)	
							n									n	Radschlupf	
							n			n	n						Antriebsleistung	
							n			n_2	n_2						Leistungssumme	
							n			n_2	n_2						zugeordnete maximale Leistung	
							n			n_2	n_2						zugeordnetes maximales Motormoment	
		b		b		b	n	b	b	b	b					n	Zugkraft (Unterlenker HKH)	Arbeitshydraulik
								n	n		n	n	n	n	n	h	Fahrersitzbelegung	
b							n			n_1	n_3						Hydraulikleistung	
							n			n_1	n_3						Pumpenfördervolumen	
h_1		h_1									n	b					hydraulischer Ölstrom	
b	h_1	h_2	h_1														hydraulischer Druck (Ventil/Pumpe)	
h_1											n	b					Ölstrom Rücklauf	
n																	Hydraulikanschlüsse gekuppelt	
h_1		h_2					n				n						hyd. Zusatzventile betätigt/Transportst.	
h_1	h_1	$h_{1/2}$	h_1								n	b					Status Zusatzventile/Schieberstellung	
			h_2														Heckkraftheber Status	
			h			b	n				n						EHR: Position/Transportverriegelung	
		$h_{1/2}$	$h_{1/2}$														Volumen aus Integration Q	
					b	h		h	h		b	b					Zapfwellendrehzahl	Zapfwelle
				h	h						b	b					Zapfwellendrehmoment	
				h		b	n			n	n						Zapfwellenleistung	
					b	h_1											Zapfwellenübersetzung	
					b	h_1	n				n						Zapfwelle Status	
					b	h_1	b	b	b	n	n	n	n	n	n	h	Zapfwellenbetätigung außen	

10 Literatur

Bücher sind mit • gekennzeichnet.

[1] Auernhammer, H.: *Präziser Ackerbau.* In: Jahrbuch Agrartechnik 16 (2004). S. 31-38, 229-230. Münster: Landwirtschaftsverlag 2004.

[2] Auernhammer, H.: *Elektronikeinsatz zur Verbesserung der landwirtschaftlichen Produktion und des Managements in der Pflanzenproduktion*. KTBL/LAV-Vortragstagung Elektronik in der Landwirtschaft Veitshöchheim 12.04.2000. In: KTBL-Schrift 390 Elektronikeinsatz in der Landwirtschaft, S. 51-58, Darmstadt: KTBL 2000.

[3] Gnahm, K.: *CAN-Bus in sicherheitsrelevanten Anwendungen*. IIR-Konferenz Landtechnische Fahrzeuge Mannheim 28./29.01.2003. Sulzbach/Ts.: IIR Deutschland GmbH 2003.

[4] -,-: *Mobile Arbeitsmaschinen – Studie Teil 1: Künftige Trends in mobilen Arbeitsmaschinen.* fluid 37 (2003) H. 9, S. 16-19.

[5] Lang, Th.: *Mechatronik in Land- und mobilen Arbeitsmaschinen.* IIR-Konferenz Landtechnische Fahrzeuge Mannheim 28./29.01.2003. Sulzbach/Ts.: IIR Deutschland GmbH 2003.

[6] Harms, H.-H.: *Stand und Entwicklungen der Hydraulik in mobilen Arbeitsmaschinen – Mechatronischer Ansatz liefert neue Lösungen.* VDMA-Nachrichten 83 (2004) H. 3, S. 60-61.

[7] •Freimann, R.: *Automation mobiler Arbeitsmaschinen – Gerät steuert Traktor.* Fortschr.-Ber. VDI Reihe 14, Nr. 116. Düsseldorf: VDI Verlag 2004.

[8] -,-: *Richtlinie 70/156/EWG des Rates vom 6. Februar 1970 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Betriebserlaubnis für Kraftfahrzeuge und Kraftfahrzeuganhänger.* Brüssel (Belgien): Rat der Europäischen Gemeinschaften 1970.

[9] -,-: *Richtlinie 2003/37/EG des Europäischen Parlaments und des Rates vom 26. Mai 2003 über die Typgenehmigung für land- oder forstwirtschaftliche Zugmaschinen, ihre Anhänger und die von ihnen gezogenen auswechselbaren Maschinen sowie für Systeme, Bauteile und selbstständige technische Einheiten dieser Fahrzeuge und zur Aufhebung der Richtlinie 74/150/EWG.* Brüssel (Belgien): Europäisches Parlament und Rat der Europäischen Union 2003.

[10] -,-: *Erdbaumaschinen – Grundtypen – Begriffe.* Norm DIN EN ISO 6165. Berlin: Beuth Verlag 2002.

[11] -,-: *Erdbaumaschinen – Grundtypen – Begriffe; Änderung A1.* Norm DIN EN ISO 6165/A1. Berlin: Beuth Verlag 2003.

[12] -,-: *Richtlinie 97/68/EG des Europäischen Parlaments und des Rates vom 16. Dezember 1997 über die Angleichung der Rechtsvorschriften der Mitgliedstaaten über Maßnahmen zur Bekämpfung der Emission von gasförmigen Schadstoffen und luftverunreinigenden Partikeln aus Verbrennungsmotoren für mobile Maschinen und Geräte.* Brüssel (Belgien): Europäisches Parlament und Rat der Europäischen Union 1997.

[13] -,-: *Straßenverkehrs-Zulassungs-Ordnung (StVZO)*. URL: http://www.stvzo.de. Wiesbaden: MORAVIA Druck + Verlag GmbH 2003.

[14] •Kunze, G., H. Göhring und K. Jacob: *Baumaschinen – Erdbau- und Tagebaumaschinen.* Braunschweig: Verlag Vieweg 2002.

[15] Pfab, H.: *Baumaschinen*. Vorlesungsunterlagen des Lehrstuhls für Landmaschinen, Technische Universität München 2003.

[16] Renius, K.Th.: *Grundlagen der Landtechnik*. Vorlesungsunterlagen des Lehrstuhls für Landmaschinen, Technische Universität München 2002.

[17] •Scheffler, M.: *Grundlagen der Fördertechnik – Elemente und Triebwerke.* Braunschweig: Verlag Vieweg 1994.

[18] Harashima, F., M. Tomizuka und T. Fukuda: *Mechatronics – "What Is It, Why and How?"*. An Editorial, IEEE/ASME Transactions on Mechatronics, Vol. 1 (1996), No. 1, S. 1-4.

[19] -,-: *UNESCO Chair On Mechatronics and Mechatronics Research and Application Center*. URL: http://mecha.ee.boun.edu.tr. UNESCO (United Nations Educational, Scientific and Cultural Organization): Paris (Frankreich) 2004.

[20] •Isermann, R.: *Mechatronische Systeme – Grundlagen.* Berlin: Springer Verlag 2002.

[21] -,-: *Entwicklungsmethodik für mechatronische Systeme.* VDI-Richtlinie VDI 2206. Berlin: Beuth Verlag 2004.

[22] •Zhang, J. (Ed.): *Automation Technology for Off-road Equipment.* Conference Proceedings Chicago, Illinois 26.-28.07.2002. St. Joseph: ASAE 2002.

[23] Höver, N. und T. Seubert: *Heutige Fahrerassistenz-Systeme und ihr Potenzial für die Zukunft.* ATZ 105 (2003) H. 10, S. 956-964.

[24] Freymann, R.: *Möglichkeiten und Grenzen von Fahrerassistenz- und Aktiven Sicherheitssystemen.* Plenarvortrag Tagung Aktive Sicherheit durch Fahrerassistenz Garching 11./12.03.2004.

[25] Marwitz, H.: *Innovationen im Nutzfahrzeug - der Weg zum Fail-Safe Truck.* Referat DaimlerChrysler Innovation Symposium 11./12.06.2002 Sindelfingen.

[26] •Walliser, G. et al.: *Elektronik im Kraftfahrzeugwesen: Steuerungs-, Regelungs- und Kommunikationssysteme.* 3. Auflage. Renningen: Expert Verlag 2002.

[27] •Bauer, H. (Chefred.): *Mikroelektronik im Kraftfahrzeug.* Technische Unterrichtung (Gelbe Reihe). Stuttgart: Robert Bosch GmbH 2001.

[28] •Bauer, H. (Chefred.): *Kraftfahrtechnisches Taschenbuch.* 23. Auflage. Braunschweig: Verlag Vieweg 1999.

[29] Rinck, St.: *Moderne hydrostatische Antriebssysteme mit Mikroprozessorsteuerungen für mobile Arbeitsmaschinen.* O+P 43 (1999) H. 3, S. 154, 157-158, 160, 162-163.

[30] Becker, A. et al.: *Integration von Fahrzeugkomponenten am Beispiel des Verkürzten Anhaltewegs.* VDI-Tagung Reifen, Fahrwerk, Fahrbahn Hannover 18./19.10.2001. In: VDI-Berichte 1632, S. 373-400. Düsseldorf: VDI Verlag 2001.

[31] Renius, K.Th. und M. Martinus: *Motoren und Getriebe bei Traktoren.* In: Jahrbuch Agrartechnik 16 (2004). S. 60-66, 234-235. Münster: Landwirtschaftsverlag 2004.

[32] •Seeger, J.: *Antriebsstrangstrategien eines Traktors bei schwerer Zugarbeit.* Diss. TU Braunschweig 2001. Forsch.-Ber. Inst. f. Landmaschinen u. Fluidtechnik TU Braunschweig. Aachen: Shaker Verlag 2001.

[33] Wiegandt, M. und H.-H. Harms: *Triebstrangmanagement bei Traktoren.* VDI-Tagung Innovative Fahrzeugantriebe Dresden 24./25.10.2002. In: VDI-Berichte 1704, S. 505-521. Düsseldorf: VDI Verlag 2002.

[34] Forche, J. und H.-H. Harms: *Management hydraulischer Antriebe in mobilen Arbeitsmaschinen.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 239-244. Düsseldorf: VDI Verlag 2003.

[35] -,-: *dlz-Neuheitenreport – Erfolgstypen mit neuer Formel.* dlz 54 (2003) H. 8, S. 74-77.

[36] Wilmer, H.: *Stufenlose Getriebe im Vergleich: Von Funktionen und Unterschieden.* profi 14 (2002) H. 7, S. 54-56.

[37] Puetz, C.: *The John Deere AutoPowr Transmission – An Infinitely Variable Transmission for Agricultural Tractors.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 25-30. Düsseldorf: VDI Verlag 2003.

[38] Münch, P., J. Hollstein, W.-D. Gruhle und Ch. Göbel: *Stufenlose Getriebe und ihr Einsatz in der modernen Landtechnik.* VDI-Tagung Steuerung und Regelung von Fahrzeugen und Motoren AUTOREG 2002 Mannheim 15./16.04.2002. In: VDI-Berichte 1672, S. 29-40. Düsseldorf: VDI Verlag 2002.

[39] Reiter, H.: *Innovative Technologien am Traktor durch Elektronikanwendung.* Landtechnik 58 (2003) H. 3 (Sonderteil Prof. Renius 65 Jahre), S. 162, 164-165.

[40] Dittrich, T., R. Hofmann und J. Ammann: *TMS-Option für individuelle Wahl der Bedienung und Fahrstrategie.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 55-59. Düsseldorf: VDI Verlag 2003.

[41] Knechtges, H.J.: *Trends bei Traktoren und Transportfahrzeugen.* Landtechnik 58 (2003) H. 6, S. 370-372.

[42] Hommel, R., R. Lutz und W. Baur: *Bewährte Getriebetechnik mit einem Höchstmaß an Komfort – Das automatisierte 4-fach-Lastschaltgetriebe mit Komfortkupplung für Same Deutz-Fahr Agrotron Traktoren.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 19-23. Düsseldorf: VDI Verlag 2003.

[43] Wilmer, H.: *Deutz-Fahr Agrotron 210: Große Klasse....* profi 15 (2003) H. 12, S. 44-46.

[44] Wiegandt, M. und H.-H. Harms: *Grundlagen eines Bremsmanagements für Traktoren.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 61-66. Düsseldorf: VDI Verlag 2003.

[45] Pandit, M.: *Steer-by-Wire – Wo stehen wir?* ATZ 101 (1999) H. 11, S. 914.

[46] Gies, St. und M. Schachner: *Neue Funktionalitäten durch elektronifizierte Lenksysteme*. 13. Aachener Kolloquium Fahrzeug- und Motorentechnik 04.-06.10.2004. In: Tagungsunterlagen Band 2, S. 1479-1500. Aachen: fka Forschungsgesellschaft Kraftfahrwesen mbh Aachen 2004.

[47] Rieger, W.: *Aktivlenkung für aktive Sicherheit.* ATZ/MTZ-Sonderausgabe Mai 2003 „System Partners“, S. 69-72.

[48] Köhn, P. et al.: *Die Aktivlenkung. Das fahrdynamische Lenksystem des neuen 5er.* ATZ/MTZ-Sonderausgabe August 2003 „Der neue BMW 5er“, S. 96-105.

[49] Neunaber, M.: *Exklusiver Fahrbericht New Holland Fast Steer: Der schnelle Dreh.* profi 15 (2003) H. 12, S. 48-49.

[50] Wilmer, H.: *Fendt-Rückfahreinrichtung von Neumaier: Mehr als eine RÜFA....* profi 15 (2003) H. 7, S. 30-31.

[51] Höner, G.: *Neue Kommunaltechnik im praktischen Einsatz.* top agrar 32 (2003) H. 6, S. 70-72.

[52] Wischhof, H.-J., E. Seidenglanz, K.-H. Gießner und A. Vogt: *Die neue Unimog-Generation. Teil I und II.* ATZ 102 (2000) H. 9, S. 686-692 und H. 10, S. 854-858, 860, 862-863.

[53] Barth, W.: *Die Aufgaben des KBA.* Vortrag Universität Bamberg. URL: http://www.kba.de/Stabsstelle/Presseservice/Schwerpunktthema/Aufgaben_desKBA2.pdf. Kraftfahrt-Bundesamt 2002.

[54] -,-: *DaimlerChrysler Powersystems auf der IAA-Nutzfahrzeuge 2002.* Bayerische Gemeindezeitung 53 (2002) Nr. 20, S. 13.

[55] Wilde, Th.: *Rübenernte - Wirkung der Großmaschine auf den Boden.* Landtechnik 53 (1998) H. 2, S. 72-73.

[56] Massak, F. und K.Th. Renius: *Mounty 65 – der neue Bergtraktor von Reform.* VDI-MEG-Tagung Landtechnik 2001 Hannover 09./10.11.2001. In: VDI-Berichte 1636, S. 41-52. Düsseldorf: VDI Verlag 2001.

[57] Ennen, J. und G. Kaupert: *Der neue Mobilkran GMK 7450. Grove-Entwicklung für den Weltmarkt.* Hebezeuge und Fördermittel 43 (2003) H. 1/2, S. 14-18.

[58] Pudszuhn, R.: *Entwicklung elektrohydraulischer Lenksysteme in der Landtechnik.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 231-238. Düsseldorf: VDI Verlag 2003.

[59] Thomsen, S. und K.B. Jensen: *Elektrohydraulische Lenkungskonzepte.* O+P 47 (2003), Nr. 10, S. 650-652.

[60] Kutzbach, H.D.: *Trends in Power and Machinery.* Journal of Agricultural Engineering Research, 76 (2000), H. 3, S. 237-247.

[61] -,-: *Lenkautomat für die Mähdrescher-Maisernte.* Landmaschinen Rundschau 27 (1975) H. 6, S. 150.

[62] • Auernhammer, H.: *Elektronik in Traktoren und Maschinen.* München: BLV Verlagsgesellschaft 1989.

[63] Diekhans, N.: *Automatische Spurführung bei Landmaschinen.* VDI-MEG-Tagung Landtechnik 2000 Braunschweig 10./11.10.2000. In: VDI-Berichte 1544, S. 337-341. Düsseldorf: VDI Verlag 2000.

[64] Rademacher, Th.: *Trends zur Verfahrenstechnik der Druschfruchternte.* Landtechnik 58 (2003) H. 6, S. 362-363.

[65] Benson, E.R., J.F. Reid, und Q. Zhang: Machine Vision-based Guidance System for Agricultural Grain Harvesters using Cut-edge Detection. Biosystems Engineering 86 (2003), H. 4, S. 389-398.

[66] Ballwieser, W. und R. Pudszuhn: *Wie ein Leitstrahl für Landmaschinen - Automatische Lenkung für Traktoren und Erntemaschinen mit Ultraschallsensoren.* Fluid 34 (2000) H. 1, S. 26, 28.

[67] Köller, K.: *Bodenbearbeitungstechnik.* In: Jahrbuch Agrartechnik 15 (2003). S. 91-97, 280. Münster: Landwirtschaftsverlag 2004.

[68] Böhrnsen, A.: *Easytronic für Aufsattelpflug von Vogel & Noot: Wenden leicht gemacht.* profi 16 (2004) H. 9, S. 66-67.

[69] Klee, U. und L. Hofmann: *DGPS-gestütztes Sicherheitssystem für Landmaschinen.* Agrartechnische Forschung 6 (2000) Heft 4, S. 80-83.

[70] Stoll, A. und H.D. Kutzbach: *Führung von Landmaschinen mit GPS.* VDI-MEG-Tagung Landtechnik 2000 Braunschweig 10./11.10.2000. In: VDI-Berichte 1544, S. 331-336. Düsseldorf: VDI Verlag 2000.

[71] Cohrs, H.H.: *Vielfalt und Hightech bei Walzenzügen.* Tiefbau, Ingenieurbau, Straßenbau 44 (2002) H. 3, S. 8-14.

[72] Engel, T. und A. Rutz: *Starfire – Das DGPS-Netzwerk von John Deere und seine Nutzung auf Landmaschinen.* VDI-MEG-Tagung Landtechnik 2002 Halle 10./11.10.2002. In: VDI-Berichte 1716, S. 293-298. Düsseldorf: VDI Verlag 2002.

[73] Holtmann, W.: *Fahrbericht Trimble AgGPS-Autopilot.* profi 15 (2003) H. 6, S. 68-70.

[74] -,-: *Traktorfahren ohne zu lenken.* Flur und Furche (John Deere) 40 (2003) H. 4, S. 5.

[75] Roberts, M.: *AutoSteer GPS 5001-Lenksystem von AutoFarm: Die etwas andere Automatiklenkung.* profi 16 (2004) H. 1, S. 76-78.

[76] Noack, P.O.: *GPS gestützte automatische Lenksysteme.* Landtechnik 59 (2004) H. 5, S. 256-257.

[77] -,-: *What is Galileo?* URL: http://www.esa.int/export/esaSA/GGGMX650NDC _navigation_0.html. European Space Agency (ESA). Paris (Frankreich): 2003.

[78] Bittner, G: *AGRO NAV Autonomous, off-road Vehicle Navigation and Implement Control System, using CDGPS and Inertial Backup.* AgEng 2000 International Conference Warwick (UK) 02.-07.07.2000. Paper 00-IE-007i. Abstracts part 1, p. 252-253.

[79] Nieminen, T.J. und M. Sampo: *Unmanned Vehicles for Agricultural and Off-Highway Applications.* SAE paper No. 932475. Society of Automotive Engineers, Warrendale, PA (USA) 1993.

[80] •Matthies, H.J. und K.Th. Renius: *Einführung in die Ölhydraulik.* 4. Auflage. Wiesbaden: Teubner Verlag 2003.

[81] Latour, Ch. und J. Beck: *Fahrantrieb und Arbeitshydraulik für Radlader.* O+P 44 (2000) Nr. 5, S. 310, 312-314, 316-317.

[82] Bönig, I.: *Kommunaltechnik.* In: Jahrbuch Agrartechnik 15 (2003). S. 233-239, 296. Münster: Landwirtschaftsverlag 2004.

[83] •Ulrich, A.: *Untersuchungen zur Fahrdynamik von Traktoren mit und ohne Anbaugeräte.* Diss. TU Berlin 1983. Forsch.-Bericht Agrartechnik d. Arbeitskreises Forschung u. Lehre der Max-Eyth-Gesellschaft (MEG) Nr. 82. Berlin: Selbstverlag 1983.

[84] Lang, Th. und H. Coenen: *Funktionspotenziale am Heckdreipunkt.* Landtechnik 55 (2000) H. 5, S. 336-337.

[85] Stewart, D: *A Platform with Six Degrees of Freedom.* Proc. Instn. Mech. Engrs. Vol. 180 (1965-66), H. 15, S. 371-378.

[86] Fedotov, S., R. Rudik, G. Bernhardt und H. Weiss: *Aufbau und Steuerung einer neuartigen Geräteschnittstelle mit zusätzlichen Freiheitsgraden.* VDI-MEG-Tagung Landtechnik 2001 Hannover 09./10.11.2001. In: VDI-Berichte 1636, S. 47-52. Düsseldorf: VDI Verlag 2001.

[87] Baldinger, M.: *Optimale Pflugarbeit mittels elektronischem Bussystem – der Elektronikpflug von Pöttinger.* VDI-MEG-Tagung Landtechnik 2001 Hannover 09./ 10.11.2001. In: VDI-Berichte 1636, S. 163-168. Düsseldorf: VDI Verlag 2001.

[88] Böhrnsen, A.: *Die elektronische Pflugsteuerung: Per Tastendruck wenden.* profi 13 (2001) H. 1, S. 70-73.

[89] -,-: Drischt am Hang wie in der Ebene. URL: http://www.deutz-fahr.de/deutsch/erntemaschinen/5670/balance.php. Lauingen: Deutz-Fahr 2003.

[90] -,-: Neue Technik macht den Hang zur Ebene. URL: http://www.claas.com/de/aktuell/berichte/produktinformationen/montana.html. Harsewinkel: Helmut Claas GmbH 2003.

[91] Ostarhild, H.: *22.176 Besucher sorgten für den unangefochtenen Messeerfolg.* Eilbote 51 (2003) H. 28, S. 8-17.

[92] Höllerl, H.: *Bergziege für Fortgeschrittene.* Forst und Technik 15 (2003) H. 8, S. 40-41.

[93] Wilmer, H: V*orgewende-Management-Systeme im Vergleich: Neues Drehen und Wenden....* profi 16 (2004), H. 2, S. 66-71.

[94] Renius, K.Th.: *Traktorenentwicklung unter besonderer Berücksichtigung der Fahrdynamik und Elektronikanwendung.* In: Fortschr.-Ber. VDI Reihe 14 Nr. 109, S. 1-24. Düsseldorf: VDI Verlag 2002.

[95] Brunotte, D. und A. Stelzer: *Traktormanagement auf dem Systemfahrzeug XERION.* VDI-MEG-Tagung Landtechnik 2001 Hannover 09./10.11.2001. In: VDI-Berichte 1636, S. 35-40. Düsseldorf: VDI Verlag 2001.

[96] Grimm, M.: *Variotronic TI – Programmierbares Vorgewendemanagement.* VDI-MEG-Tagung Landtechnik 2002 Halle 10./11.10.2002. In: VDI-Berichte 1716, S. 299-304. Düsseldorf: VDI Verlag 2002.

[97] -,-: *dlz-Neuheitenreport – Erfolgstypen mit neuer Formel.* dlz 54 (2003) H. 8, S. 74-77.

[98] -,-: *Comfortip: Individualität serienmäßig.* URL: http://www.deutz-fahr.de/deutsch/traktoren/agrotronttv/comfortip.php.

[99] Wilmer, H.: *Deutz-Fahr Agrotron TTV 1160: Stufenloser Start in Stufen.* profi 15 (2003) H. 4, S. 10-17.

[100] •Duluschitz, R. und J. Spilke (Hrsg.): *Agrarinformatik.* Stuttgart: Verlag Eugen Ulmer 2002.

[101] Bak, Th. und H. Jakobsen: *Agricultural Robotic Platform with Four Wheel Steering for Weed Detection.* Biosystems Engineering 87 (2004), H. 2, S. 125-136.

[102] Hoepke, E.: *Die IAA Nutzfahrzeuge in Hannover September 2002.* ATZ 104 (2002) H. 9, S. 760, 762-763.

[103] Kunert, M. und A. Kretzschmar: *Fahrzeugrundumsicht mit Radartechnik – Konzepte und Systeme.* VDI-Tagung Elektronik im Kraftfahrzeug 2000 Baden-Baden 05./06.10.2000. In: VDI-Berichte 1547, S. 877-895. Düsseldorf: VDI Verlag 2000.

[104] Adomat, R.: *Fahrerassistenzsysteme: Das Auto lernt sehen.* IIR-Konferenz Landtechnische Fahrzeuge Mannheim 28./29.01.2003. Sulzbach/Ts.: IIR Deutschland GmbH 2003.

[105] Wehner, U., K. Unger, K. Schulze und R. Zschoppe: *Aufbau und Auslegung eines Lane Keeping Systems.* VDI-Tagung Elektronik im Kraftfahrzeug 2003 Baden-Baden 25./26.09.2003. In: VDI-Berichte 1789, S. 339-349. Düsseldorf: VDI Verlag 2003.

[106] Labahn, N.: *Anwendung eines neuen induktiven Messprinzips zur Realisierung kontaktloser Winkel- und Positionssensoren*. VDI-MEG-Tagung Landtechnik 2004 Dresden 07./08.10.2004. In: VDI-Berichte 1855, S. 99-106. Düsseldorf: VDI Verlag 2004.

[107] Dorißen, H.Th. und K. Dürkopp: *Räumliche und funktionale Integration von kontaktlosen Positionssensoren für X-by-Wire-Systeme.* VDI-Tagung Mechatronik Fulda 07./08.05.2003. In: VDI-Berichte 1753, S. 129-143. Düsseldorf: VDI Verlag 2003.

[108] •Bauer, H. (Chefred.): *Sensoren im Kraftfahrzeug.* Technische Unterrichtung (Gelbe Reihe). Stuttgart: Robert Bosch GmbH 2001.

[109] Hlubek, B. und D. Hobein: *Intelligente Sensorik - Basis für Perfekte Performance.* ATZ 102 (2000) Heft 12, S. 1118-1123.

[110] Fischle, G., U. Stoll und W. Hinrichs: *Bremsen auf höchstem Niveau – Die Sensorik Brake Control.* ATZ/MTZ-Sonderausgabe Mai 2002 „Die neue Mercedes-Benz E-Klasse“, S. 142-144, 146, 148-150.

[111] Leohold, J.: *Die elektrische Infrastruktur für zukünftige Fahrerassistenzsysteme.* 5. Braunschweiger Symposium Automatisierungs- und Assistenzsysteme für Transportmittel Braunschweig 17./18.02.2004.

[112] Hieronymus, P., R. Buschmeier, S. Böttinger: *Kommunikationssysteme.* In: Jahrbuch Agrartechnik 16 (2004). S. 38-43, 230. Münster: Landwirtschaftsverlag 2004.

[113] •Etschberger, K.: *CAN Controller Area Network- Grundlagen, Protokolle, Bausteine, Anwendungen.* 2. Auflage. München: Carl Hanser Verlag 2000.

[114] Brunotte, D. und J. Seeger: *Kommunikation von Motor und Getriebe über CAN-Bus.* Agrartechnische Forschung 5 (1999) H. 1, S. 54-67.

[115] Hofmann, R.: *Traktorelektronik neue Generation: Konzept und Realisierung am Beispiel des Fendt Favorit 700.* VDI-MEG-Tagung Landtechnik 1999 Braunschweig 7./8.10.1999. In: VDI-Berichte 1503, S. 75-80. Düsseldorf: VDI Verlag 1999.

[116] -,-: *Recommended Practice for a Serial Control and Communications Vehicle Network.* Norm SAE J1939. Berlin: Beuth Verlag 2003.

[117] -,-: *Traktoren und Maschinen für die Land- und Forstwirtschaft – Serielles Kontroll- und Kommunikationsnetzwerk.* Normentwurf ISO 11783. Berlin: Beuth Verlag 2003.

[118] •Goering, C.E., M.L. Stone, D.W. Smith und P.K. Turnquist: *Off-Road Vehicle Engineering Principles.* St. Joseph (USA): ASAE 2003.

[119] Thomas, R.: *ISOBUS in der Kommunaltechnik.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 115-119. Düsseldorf: VDI Verlag 2003.

[120] -,-: *Industrielles Kommunikationssubsystem basierend auf ISO 11898 (CAN) – Teil 4: CANopen.* Norm DIN EN 50325-4. Berlin: Beuth Verlag 2002.

[121] Unger, E., H. Witte und W. Poppy: *CANopen in mobilen Baumaschinen.* 2. Internationales Fluidtechnisches Kolloquium in Dresden 16./17.03.2000. In: Tagungsunterlagen Band 2, S. 105-112. Dresden: Dresdner Verein zur Förderung der Fluidtechnik 2000.

[122] -,-: *Straßenfahrzeuge – Diagnosesysteme – Schlüsselwort 2000.* Norm ISO 14230. Berlin: Beuth Verlag 2000.

[123] -,-: *Recommended Practice for a Serial Control and Communications Vehicle Network – Application Layer Diagnostics.* Norm SAE J1939/73. Berlin: Beuth Verlag 2001.

[124] -,-: *Road Vehicles – Diagnostics on Controller Area Networks (CAN).* Normentwurf ISO/DIS 15765. Berlin: Beuth Verlag 2003.

[125] Schlingmann, N.: *Diagnose im Feldeinsatz bei CLAAS.* VDI-MEG-Tagung Landtechnik 2004 Dresden 07./08.10.2004. In: VDI-Berichte 1855, S. 145-150. Düsseldorf: VDI Verlag 2004.

[126] -,-: *Straßenfahrzeuge - Austausch digitaler Informationen - Steuergerätenetz (CAN) für schnellen Datenaustausch.* Norm ISO 11898. Berlin: Beuth Verlag 2003.

[127] Führer, Th. et al.: *TTCAN: Zeitgesteuerter Nachrichtenverkehr im CAN-Netzwerk.* VDI-Tagung Elektronik im Kraftfahrzeug 2001 Baden-Baden 27./28.09.2001. In: VDI-Berichte 1646, S. 43-52. Düsseldorf: VDI Verlag 2001.

[128] Plankensteiner, M., St. Poledna und G. Stöger: *Das zeitgesteuerte Protokoll TTP.* ATZ/MTZ/Automotive Engineering Partners Sonderausgabe September 2002 „Automotive Electronics“, S. 60-63.

[129] -,-: *Time-Triggered Protocol TTP/C High-Level Specification Document Protocol Version 1.1.* URL: http://www.tttech.com. Wien (Österreich): TTTech Computertechnik AG 2003.

[130] Heinecke, H. et al.: *FexRay – ein Kommunikationssystem für das Automobil der Zukunft.* Elektronik Sonderheft Automotive September 2002, S. 36-40, 42-45.

[131] -,-: *FlexRay Communications System Protocol Specification Version 2.0.* URL: http://www.flexray-group.com. FlexRay Consortium 2004.

[132] Neumayer, R. et al.: *Kommunikationsstruktur und Bordnetz des neuen BMW 5er.* ATZ/MTZ-Sonderausgabe August 2003 „Der neue BMW 5er“, S. 106-107, 108, 110, 112, 114.

[133] Albert, A. und A. Trächtler: *Verteilte Fahrdynamikregelung mit zeitgesteuerter Architektur am Beispiel des Bosch-Konzeptes VDM.* 13. Aachener Kolloquium Fahrzeug- und Motorentechnik 04.-06.10.2004. In: Tagungsunterlagen Band 1, S. 593-610. Aachen: fka Forschungsgesellschaft Kraftfahrwesen mbh Aachen 2004.

[134] Versmold, H. und T. Gleissner: *Einfluss des Technologiewandels auf die zukünftige Gestaltung von Fahrzeugelektronik und Systemarchitekturen.* 13. Aachener Kolloquium Fahrzeug- und Motorentechnik 04.-06.10.2004. In: Tagungsunterlagen Band 2, S. 1591-1605. Aachen: fka Forschungsgesellschaft Kraftfahrwesen mbh Aachen 2004.

[135] Anderl, Th.: *Entwicklung und Absicherung der CAN-Kommunikation des Münchner Autarken Hybrids mit modellbasierten HIL Simulation.* VDI-MEG-Tagung Simulation und Simulatoren – Mobilität virtuell gestalten – Hamburg 15./16.04.2003. In: VDI-Berichte 1745, S. 321-342. Düsseldorf: VDI Verlag 2003.

[136] Torlo, M. und T. Bertram: *Dynamische, verteilte Fehlertoleranz in vernetzten Kraftfahrzeugsystemen.* VDI-Tagung Elektronik im Kraftfahrzeug 2001 Baden-Baden 27./28.09.2001. In: VDI-Berichte 1646, S. 99-122. Düsseldorf: VDI- Verlag 2001.

[137] -,-: *Das V-Modell – Planung und Durchführung von IT-Vorhaben – Entwicklungsstandard für IT-Systeme des Bundes.* URL: http://www.v-modell.iabg.de. München: IABG mbH 2003.

[138] Mutz, M. et al.: *Ein durchgehender modellbasierter Entwicklungsprozess für elektronische Systeme im Automobil.* VDI-Tagung Elektronik im Kraftfahrzeug 2003 Baden-Baden 25./26.09.2003. In: VDI-Berichte 1789, S. 43-75. Düsseldorf: VDI Verlag 2003.

[139] -,-: *Informationstechnik – Bewertung von Software-Prozessen.* Norm ISO/IEC 15504. Berlin: Beuth Verlag 2004.

[140] -,-: *Welcome to the CMMI Web Site.* URL: http://www.sei.cmu.edu/cmmi. Software Engineering Institute. Pittsburgh (USA): Carnegie Mellon University 2003.

[141] -,-: *Richtlinie 98/37/EG des europäischen Parlamentes und des Rates vom 22. Juni 1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen (Maschinenrichtlinie).* Brüssel (Belgien): Kommission der Europäischen Gemeinschaften 2001.

[142] -,-: *Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 03. Dezember 2001 über die allgemeine Produktsicherheit.* Brüssel (Belgien): Europäisches Parlament und Rat der Europäischen Union 2001.

[143] Klindt, Th.: *Bedeutung der EG-Maschinenrichtlinie für Landmaschinen-Hersteller.* Landtechnik 58 (2003) H. 4, S. 258-259.

[144] -,-: *Richtlinie 71/320/EWG des Rates vom 26. Juli 1971 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Bremsanlagen bestimmter Klassen von Kraftfahrzeugen und deren Anhängern.* Brüssel (Belgien): Europäisches Parlament und Rat der Europäischen Union 2001.

[145] -,-: *Richtlinie 70/311/EWG des Rates vom 8. Juni 1970 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Lenkanlagen von Kraftfahrzeugen und Kraftfahrzeuganhängern.* Brüssel (Belgien): Europäisches Parlament und Rat der Europäischen Union 1999.

[146] -,-: *Richtlinie 75/321/EWG des Rates vom 20. Mai 1975 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Lenkanlage von land- oder forstwirtschaftlichen Zugmaschinen auf Rädern.* Brüssel (Belgien): Europäisches Parlament und Rat der Europäischen Union 1998.

[147] -,-: *Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze.* Norm DIN EN ISO 12100. Berlin: Beuth Verlag 2003.

[148] -,-: S*icherheit von Maschinen – Leitsätze zur Risikobeurteilung.* Norm ISO 14121. Berlin: Beuth Verlag 1999.

[149] -,-: *Leittechnik; Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen.* Vornorm DIN V 19250. Berlin: Beuth Verlag 1994.

[150] -,-: *Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur gesicherten Funktion.* Vornorm DIN V 19251. Berlin: Beuth Verlag 1995.

[151] -,-: *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.* Norm DIN EN 61508. Berlin: Beuth Verlag 2001.

[152] -,-: *Sicherheit von Maschinen – Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren Steuerungen von Maschinen.* Norm-Entwurf DIN IEC 62061. Berlin: Beuth Verlag 2003.

[153] -,-: *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen.* Norm DIN EN ISO 13849. Berlin: Beuth Verlag 2003.

[154] -,-: *Land- und forstwirtschaftliche Maschinen – Elektromagnetische Verträglichkeit – Prüfverfahren und Bewertungskriterien.* Norm DIN EN ISO 14982. Berlin: Beuth Verlag 1998.

[155] -,-: *Erdbaumaschinen – Maschinensteuerungssysteme (MSS) auf der Basis von elektronischen Bauteilen – Anforderungen und Prüfungen.* Normentwurf ISO/DIS 15998, Arbeitsgruppe ISO/TC 127/SC 3. Berlin: Beuth Verlag 2004.

[156] -,-: *Agricultural engineering – Electrical and electronical equipment – Testing resistance to environmental conditions.* Normentwurf ISO/DIS 15003, Arbeitsgruppe ISO TC 23/SC 19/WG 1. Berlin: Beuth Verlag 2004.

[157] -,-: *Straßenfahrzeuge - Umgebungsbedingungen und Prüfungen von elektrischer und elektronischer Ausrüstung.* Norm ISO 16750. Berlin: Beuth Verlag 2003.

[158] -,-: *Richtlinie 75/322/EWG des Rates vom 20. Mai 1975 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Funkentstörung der Fremdzündungsmotoren von land- oder forstwirtschaftlichen Zugmaschinen auf Rädern.* Brüssel (Belgien): Europäisches Parlament und Rat der Europäischen Union 2000.

[159] -,-: *Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen.* Norm DIN EN 60204-1. Berlin: Beuth Verlag 2001.

[160] -,-: *Sicherheitstechnische Begriffe für Automatisierungssysteme.* VDI-Richtlinie VDI/VDE 3542. Berlin: Beuth Verlag 2000.

[161] •Echtle, K.: *Fehlertoleranzverfahren.* Berlin: Springer Verlag 1990.

[162] •Ehrlenspiel, K.: *Integrierte Produktentwicklung.* 2. Auflage. München: Carl Hanser Verlag 2003.

[163] -,-: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen. Norm DIN EN 954. Berlin: Beuth Verlag 1997.

[164] -,-: *Qualitätsmanagement in der Automobilindustrie, Sicherung der Qualität vor Serieneinsatz, Teil 4.2, System-FMEA.* Norm VDA 4.2. Frankfurt/M.: Verband der Automobilindustrie e.V. (VDA) 1996.

[165] Loos, S.: *Systemanalyse Risikoanalyse mit der Methode FMEA nach VDA-4 Teil 2.* Seminarunterlage. Düsseldorf: VDI Bildungswerk 1999.

[166] -,-: *TQE – Total Quality Engineering.* URL: http://www.plato-ag.com. Lübeck: PLATO AG 2004.

[167] -,-: *APIS Informationstechnologien GmbH.* URL: http://www.apis.de. Wörth/ Donau: APIS Informationstechnologien GmbH 2004.

[168] • Goble, W.M.: *Control Systems Safety Evaluation & Reliability.* 2. Auflage. NC (USA): ISA – The Instumentation, Systems, and Automation Society 1998.

[169] -,-: *Projektwirtschaft – Projektabwicklung – Begriffe.* Norm DIN 69905. Berlin: Beuth Verlag 1997.

[170] • Yourdon, E.: *Moderne Strukturierte Analyse.* Attenkirchen: Wolfram‘s Fachverlag 1992.

[171] Beer, A.: *X-by-Wire: Von der Entwicklung zur Einführung.* ATZ/MTZ/Automotive Engineering Partners Sonderausgabe März 2001 „Automotive Electronics“, S. 80-85.

[172] Peng, W. und D. Wallace: *Software Error Analysis.* National Institute of Standards and Technology (NIST), Special Publication 500-209. Gaithersburg 1993.

[173] -,-: *Programmiersprachen – C.* Norm ISO/IEC 9899. Berlin: Beuth Verlag 2001.

[174] Thomsen, T.: *Integration automotiver Standards in die Seriencodegenerierung.* VDI-Tagung Steuerung und Regelung von Fahrzeugen und Motoren AUTOREG 2002 Mannheim 15./16.04.2002. In: VDI-Berichte 1672, S. 205-221. Düsseldorf: VDI Verlag 2002.

[175] -,-: *Entwicklungsempfehlungen für Software von Straßenfahrzeugen.* Technical Report ISO/TR 15497, Berlin: Beuth Verlag 2000.

[176] Schwarz, H., H. Deiss und H. Lier: *Prozess-Management in der industriellen Software-Produktion.* VDI-Tagung Elektronik im Kraftfahrzeug 2000 Baden-Baden 05./06.10.2000. In: VDI-Berichte 1547, S. 371-389. Düsseldorf: VDI Verlag 2000.

[177] Waldmann, A.: *Kontrollierte Software-Updates von elektronischen Fahrzeug-Steuergeräten.* VDI-MEG-Tagung Landtechnik 2004 Dresden 07./08.10.2004. In: VDI-Berichte 1855, S. 131-136. Düsseldorf: VDI Verlag 2004.

[178] -,-: *The MathsWorks Worldwide.* URL: http://www.mathworks.com. Natick (USA): The MathWorks, Inc. 2004.

[179] Wohnhaas, A. und H.-J. Habrock: *Szenarien und Schritte bei der Einführung modellbasierter Methoden in der Kfz-Elektronikentwicklung.* VDI-Tagung Elektronik im Kraftfahrzeug 2000 Baden-Baden 05./06.10.2000. In: VDI-Berichte 1547, S. 327-345. Düsseldorf: VDI Verlag 2000.

[180] -,-: *Telelogic – Requirements Driven Innovation.* URL: http://www.telelogic.com. Malmö (Schweden): Telelogic AB 2004.

[181] Kokes, M. und A. von Querfurth: *Methodik zur Spezifikation von Elektronik im Fahrzeug.* VDI-Tagung Elektronik im Kraftfahrzeug 2001 Baden-Baden 27./ 28.09.2001. In: VDI-Berichte 1646, S. 169-179. Düsseldorf: VDI Verlag 2001.

[182] -,-: *dSPACE – Solutions for Control.* URL: http://www.dspace.com. Paderborn: dSPACE GmbH 2004.

[183] Otterbach, R., M. Eckmann und F. Mertens: *Rapid Control Prototyping – neue Möglichkeiten und Werkzeuge.* VDI-Tagung Steuerung und Regelung von Fahrzeugen und Motoren AUTOREG 2004 Wiesloch 02./03.03.2004. In: VDI-Berichte 1828, S. 527-538, Düsseldorf: VDI Verlag 2004.

[184] Jungmann, M. und M. Beine: *Automatische Code-Generierung für sicherheitskritische Systeme.* ATZ/MTZ/Automotive Engineering Partners Sonderausgabe September 2003 „Automotive Electronics“, S. 50-55.

[185] Junker, F., I. Mohr und J. Schreiber: *Durch TÜV bestätigt – Hoher Qualitätsanspruch des ASCET-SD-Codegenerators.* ATZ/MTZ/Automotive Engineering Partners Sonderausgabe September 2003 „Automotive Electronics“, S. 61-63.

[186] • Spitzer, B.: *Modellbasierter Hardware-in-the-Loop Test von eingebetteten elektronischen Systemen*. Diss. Universität Karlsruhe, Fakultät für Elektrotechnik und Informationstechnik 2001.

[187] Wältermann, P., H. Schütte und K. Diekstall: *Hardware-in-the-Loop-Test verteilter Kfz-Elektroniksysteme.* ATZ 106 (2004) H. 5, S. 416-425.

[188] Keinath A., M. Pillin und K. Lebert: *Modulare Testumgebung für verschiedene Systemebenen und Prozessphasen*. ATZ/MTZ/Automotive Engineering Partners Sonderausgabe März 2004 „Automotive Electronics“, S. 22-25.

[189] Kirrmann, H. und K.-E. Großpietsch: *Fehlertolerante Steuerungs- und Regelungssysteme*. Automatisierungstechnik 50 (2002) H. 8, S. 362-374.

[190] • Schäuffele, J. und Th. Zurawka: *Automotive Software Engineering – Grundlagen, Prozesse, Methoden und Werkzeuge.* Wiesbaden: Verlag Vieweg 2003.

[191] -,-: *Informationsverarbeitung; Sinnbilder und ihre Anwendung.* Norm DIN 66001. Berlin: Beuth Verlag 1983.

[192] Heißing, B.: *Dynamik der Straßenfahrzeuge.* Vorlesungsunterlagen des Lehrstuhls für Fahrzeugtechnik, Technische Universität München 2004.

[193] -,-: *LSV – Die Landwirtschaftliche Sozialversicherung.* URL: http://www.lsv.de, Kassel: Spitzenverbände der landwirtschaftlichen Sozialversicherung 2004.

[194] Rüb, W.: *Vielseitiger Ventilbaukasten mit Wahlmöglichkeiten von einfacher Ausstattung bis zu Multifunktionsventilen mit CAN-Elektronik.* VDI-MEG-Tagung Landtechnik 2003 Hannover 07./08.11.2003. In: VDI-Berichte 1798, S. 225-230. Düsseldorf: VDI Verlag 2003.

[195] Fertig, G.: *LUDV-Steuerungen.* Fachtagung Antriebs- und Steuerungssysteme für moderne Mobilmaschinen, Mannesmann Rexroth AG Lohr a. Main, Nov. 1994.

[196] • Theis, I.: *Das Steer-by-Wire System im Kraftfahrzeug – Analyse der menschlichen Zuverlässigkeit.* Diss. TU München, Fakultät für Maschinenwesen 2002.